ENM Configuration Troubleshooting Guide

Check List

1/159 01-AOM 901 151-1 Uen CA

Copyright

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Contents

1 ENM Configuration Troubleshooting Guide

This document describes the troubleshooting tasks for the ENM Configuration applications.

Target Group

System Administrators.

2 Connect to a Virtual Machine

> To connect to the virtual machine (VM) linked to the deployment, determine what environment you are working on and follow the task relevant to your environment.

2.1 Connect to a Virtual Machine on a Physical ENM Deployment

Prerequisites

A command window is open and you have `superuser` privileges.

Steps

1. Log on to the ENM MS as **`litp-admin`** user and switch to the **`root`** user.
2. List the contents of the host file to view all connected VMs within the deployment.

```
[root@ms-1 ~]# cat /etc/hosts
...
192.168.99.20 svc-1-pmserv # Created by LITP. Please do not edit
192.168.99.26 svc-1-netex # Created by LITP. Please do not edit
192.168.99.16 svc-1-ebc # Created by LITP. Please do not edit
192.168.99.36 svc-1-mspm # Created by LITP. Please do not edit
192.168.99.28 svc-1-uiserv # Created by LITP. Please do not edit
192.168.99.14 svc-1-supervc # Created by LITP. Please do not edit
...
192.168.99.32 svc-1-mscm # Created by LITP. Please do not edit
...
192.168.99.50 svc-1-jms # Created by LITP. Please do not edit
...
192.168.99.3 logstash # Created by LITP. Please do not edit
...
192.168.99.2 httpd # Created by LITP. Please do not edit
192.168.99.40 sso # Created by LITP. Please do not edit
...
192.168.99.12 svc-1-medrout # Created by LITP. Please do not edit
192.168.99.22 svc-1-cmserv # Created by LITP. Please do not edit
192.168.99.52 svc-1-sec # Created by LITP. Please do not edit
192.168.99.8 openidm # Created by LITP. Please do not edit
```

   The aliases for the parallel VMs take the form of `<SVC host>-<service>`.

   For example: `svc-1-cmserv, svc-2-cmserv`.

   The active-passive VMs take the form of `<service>`.

   For example: `httpd, sso, openidm`.

3. To access the VM, copy the private key of the cloud-user from its secure location to the `MS` or `SVC` node.

```
[root@ms-1 ~]# /root/.ssh/vm_private_key
```

Refer to *VM Security Tasks* in the *ENM System Administrator Guide* to learn more about the `vm_private_key`.

4. Connect by `SSH` to the VM you want.

   To access the `VM`, use the `cloud-user` user ID and include the path to the `VM` private key. For example:

```
[root@ms-1 ~]# ssh -i /root/.ssh/vm_private_key cloud-user@svc-1-cmserv
Last login: Thu Feb 26 10:14:43 2015 from 192.110.0.59
[cloud-user@svc-1-cmserv ~]# sudo su - root
[root@svc-1-cmserv ~]#
```

2.2 Connect to a Virtual Machine on an ENM on Cloud Deployment

Prerequisites

— A command window is open and you have `superuser` privileges.

— You have access to the private key file for authentication, contact your OpenStack administrator

Steps

1. List the virtual machine aliases from the consul service:

   Using the private key for authentication, copy the key to the EMP server. Log on to EMP server and list the consul members to view all connected VMs within the deployment:

```
> scp -i <cloud-user private key> <cloud-user private key> cloud-user@<EMP I →
P Address>:/var/tmp/vm_private_key
> ssh -i <cloud-user private key> cloud-user@<EMP IP Address>
[cloud-user@ostk003-emp-0 ~]$ chmod 700 /var/tmp/vm_private_key
[cloud-user@ostk003-emp-0 ~]$ sudo su -
[root@ostk003-emp-0 ~]# consul members
Node                       Address          Status  Type    Build  Protocol  →
 DC
haproxy                    10.3.2.31:8301   alive   client  0.8.1  2         →
 dc1
opendj-1                   10.3.2.83:8301   alive   client  0.8.1  2         →
 dc1
opendj-2                   10.3.2.84:8301   alive   client  0.8.1  2         →
 dc1
openidm                    10.3.2.85:8301   alive   client  0.8.1  2         →
 dc1
ostk003-accesscontrol-0    10.3.1.251:8301  alive   client  0.8.1  2         →
 dc1
ostk003-accesscontrol-1    10.3.1.252:8301  alive   client  0.8.1  2         →
 dc1
ostk003-elasticsearch-0    10.3.2.15:8301   alive   client  0.8.1  2         →
 dc1
...
ostk003-neo4j-2            10.3.2.77:8301   alive   client  0.8.1  2         →
 dc1
```

```
ostk003-nfscommon-0        10.3.0.81:8301   alive   client  0.8.1  2          →
 dc1
ostk003-nfsnrbk-0          10.3.0.83:8301   alive   client  0.8.1  2          →
 dc1
ostk003-nfspm-0            10.3.0.85:8301   alive   client  0.8.1  2          →
 dc1
ostk003-nfspm-1            10.3.0.82:8301   alive   client  0.8.1  2          →
 dc1
...
ostk003-secserv-1          10.3.2.98:8301   alive   client  0.8.1  2          →
 dc1
ostk003-serviceregistry-0  10.3.2.100:8301  alive   server  0.8.1  2          →
 dc1
ostk003-serviceregistry-1  10.3.2.101:8301  alive   server  0.8.1  2          →
 dc1
ostk003-serviceregistry-2  10.3.2.102:8301  alive   server  0.8.1  2          →
 dc1
ostk003-uiserv-0           10.3.2.116:8301  alive   client  0.8.1  2          →
 dc1
ostk003-uiserv-1           10.3.2.117:8301  alive   client  0.8.1  2          →
 dc1
ostk003-vnflaf-services    10.3.1.249:8301  alive   client  0.8.1  2          →
 dc1
...
svc-2-httpd                10.3.2.35:8301   alive   client  0.8.1  2          →
 dc1
svc-2-sps                  10.3.2.111:8301  alive   client  0.8.1  2          →
 dc1
svc-2-sso                  10.3.2.113:8301  alive   client  0.8.1  2          →
 dc1
```

2. SSH to the VM you want.

   To access the VM, use the cloud-user user ID and include the path to the VM private key. The VM can be accessed using either the node identifier or it's IP address. For example:

```
[cloud-user@ostk003-emp-0 ~]$ ssh -i /var/tmp/vm_private_key cloud-user@10.3 →
.2.31
The authenticity of host 'haproxy (10.3.2.31)' can't be established.
RSA key fingerprint is b9:4f:ca:4f:bc:55:00:de:a8:77:e5:08:56:7c:db:98.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'haproxy,10.3.2.31' (RSA) to the list of known ho →
sts.
[cloud-user@haproxy ~]$
```

3 CM Node Synchronization Troubleshooting - MINI-LINK Indoor Nodes

> This section provides troubleshooting steps to diagnose common problems with node synchronization and notification handling of MINI-LINK-Indoor nodes.

Collecting system logs

SNMP CM synchronization generates log messages during operation, which can help users find out the root cause for a failure. For troubleshooting purposes, logs can be accessed with the Log Viewer application (of level WARN and error) or from the Management Server (of level INFO, WARN and ERROR by default)

Accessing logs with Log Viewer application

Open the Log Viewer application and search for the name of the Network element, if needed, combine the search with some more specific keywords from the log message. For more information, see *Log Viewer Description* in *ENM Product Description*.

Accessing logs through the Management Server

1. Log on to the ENM MS as the **litp-admin** user and switch to **root** user.
2. Check all Mediation Service for SNMP Configuration Management (MSSNMPCM) JBoss logs using the following command:

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mssnmpcm\s" →
 | awk '{print $2}'); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep -i "<log keyword to search>\|<other log keyword to search>" →
\
/ericsson/3pp/jboss/standalone/log/server.log*'| grep -i <Nod →
eName>'; done

Logging into svc-2-mssnmpcm
2017-06-21 10:09:48,521 ERROR <some error messages>
...
[root@ms-1 ~]#
```

Substitute the list of keywords and the node name, extend if needed.

3.1 Attempt Manual Sync when CM Node Supervision is Deactivated for MINI-LINK Indoor

Each node that is managed by ENM has an attribute called `CmNodeHeartbeatSupervision.active`. This attribute can be set to `true` or `false` to notify ENM that the node is targeted for supervision or not. Only supervised nodes can be synchronized with ENM.

Prerequisites

— Basic knowledge of how to use the CM CLI.

Steps

1. If the CM supervision of the node is deactivated and a manual synchronization of the node is triggered in the CM CLI, the synchronization status of the node will be set to UNSYNCHRONIZED and an error similar to the below will be displayed.

```
»cmedit action NetworkElement=TN100,CmFunction=1 sync

FAILED FDN : NetworkElement=TN100,CmFunction=1
Error 9999 : Internal Error The operation was reverted because of a system error (Node ID: svc-2-mssnmpcm. Exception occurred: CM heartbeat supervision is disabled,
can't synchronize 'NetworkElement=TN100'.)
```

2. Check if the CM supervision is deactivated for the node, and then activate it.

```
1)     cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    active : false

    1 instance(s)

2)     cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1 act →
ive=true
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1

    1 instance(s)
```

3. Supervision of the node will automatically be triggered in ENM once the value of `CmNodeHeartbeatSupervision.active` changes state from `false` to `true`. It may take some time for the node to synchronize. Execute the below command until the node state changes to SYNCHRONIZED.

```
1)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : SYNCHRONIZED

    1 instance(s)
```

Results

The node is synchronized with ENM

3.2 MINI-LINK Indoor Node Unreachable from ENM

To synchronize with a node, ENM must have a physical connection and the correct network settings between the node and ENM.

The node may be unreachable from ENM for one of the following reasons:

1. ENM specific ports are not available. Refer to page 296.
2. Network connectivity to the node is faulty.
3. The node is stopped, not responding or in an error state.

   Refer to the *Troubleshooting Guide* in the CPI delivered with the relevant node.
4. The security configuration is invalid or incorrect, and permission is denied during SNMP communication handshake between ENM and the node.

Prerequisites

— Root access to the Management Server (MS).

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the CM CLI.

Steps

1. If the node that ENM is attempting to synchronize with is unreachable, sync status will be set to UNSYNCHRONIZED. To check this run the following commands from the CM CLI

```
1)    cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)

2)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. To confirm that the node is unreachable, the JBOSS logs need to be checked. Check the logs for the following:

Level	Log message(s)	Meaning	Actions
WARN	`Heartbeat unsuccessful for '<NE_FDN>', could be a configuration problem`	Node was not responding on SNMP, can be unreachable or connection attributes may be incorrect	Check that the node is reachable and verify the configuration and and change the incorrect values. To set or update credentials,

Level	Log message(s)	Meaning	Actions
			refer to *Create Node Credentials* in the page 296.

Example

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mssnmpcm\s" | awk '{print
$2}'); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "Heartbeat unsuccessful" \
/ericsson/3pp/jboss/standalone/log/server.log* | grep <NodeName>'; done
Logging into svc-2-mssnmpcm
2016-10-19 10:04:18,937 INFO  [com.ericsson.oss.mediation.minilinkindoor.cm.
operation.HeartBeatMDBean] (default-threads - 2)  HEARTBEAT EVENT in MDB ---
-------> com.ericsson.oss.mediation.adapter.heartbeat.connector.api.HbStatus
Event@1866564139[resourceKey: NetworkElement=<NodeName>, timestamp: 14768678
56631, HbState: OUT_OF_SERVICE]
```

Results

Possible root causes of synchronization failure identified.

3.3 Troubleshoot MINI-LINK Indoor Node Synchronization Failure at First Attempt

The first time ENM attempts to synchronize a node, it must calculate the node model identity by reading the Administrative Data (neProductVersion) from the node.

If this operation fails, it looks for the `ossModelIdentity` supplied by the operator and uses it to synchronize the node.

If also the `ossModelIdentity` is not present or it is not a valid value, the node cannot be synchronized.

This guide provides information on steps to identify and troubleshoot this issue.

Prerequisites

— Root access to the management server or access to Log Viewer application.

— Basic knowledge of Linux and JBoss.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Verify that the node synchronization is activated and the sync status is UNSYNCHRONIZED. Execute the commands:

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)
```

```
2)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. Verify the `neProductVersion` is not set executing the command:

```
cmedit get <NodeName> NetworkElement.neProductVersion
FDN : NetworkElement=<NodeName>
neProductVersion : null

1 instance(s)
```

3. One of the reasons the `neProductVersion` is not set is because the node is unreachable.

   To verify and troubleshoot this case, please refer to MINI-LINK Indoor Node Unreachable from ENM

4. In case the node is reachable, verify if the security credentials are correctly set.

   Look for the following log messages (you may use the bold parts as search phrases):

Level	Log message(s)	Meaning	Actions
WARN	`Can't synchronize '<NE FDN>' because the OSS model identity is not known.`	`ossModelIdentity` can not be populated automatically	Set the `ossModelIdentity` attribute to a compatible value

ERROR
ERROR
WARN
	`Configuration for '<NE FDN>' is inconsistent or could not decide the privacy protocol from '<some value>'`
	`Configuration for '<NE FDN>' is inconsistent or could not decide the auth protocol from '<some value>'`
	`Attribute <name of attribute> was empty for <NES FDN>`
		Some values are missing from the configuration.	Verify the configuration and and set the missing values. To set or update credentials, refer to *Create Node Credentials* in the page 296.

WARN	`Heartbeat unsuccessful for '<NE_FDN>', could be a configuration problem`	Node was not responding on SNMP, can be unreachable or connection attributes may be incorrect	Verify the configuration and and change the incorrect values. To set or update credentials, refer to *Create Node Credentials* in the page 296.

Example

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mssnmpcm\s" | awk '{print →
$2}'); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep -i "is inconsistent or could not\|because the OSS model identity is no →
t known\|was empty for\|could be a configuration problem" \
/ericsson/3pp/jboss/standalone/log/server.log*'; done

Logging into svc-2-mssnmpcm
Caused by: com.ericsson.oss.mediation.cm.snmp.exception.DpsRuntimeException: →
 Configuration for 'NetworkElement=MINI-LINK-Indoor-02' is inconsistent or c →
```

```
ould not decide the privacy protocol from 'NONE'
[root@cloud-ms-1 ~]#
```

5. Force the synchronization of the node by running a manual sync command:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 sync
FDN : NetworkElement=<NodeName>,CmFunction=1

1 instance(s)
```

6. It may take some time for the node to synchronize. Repeat,until the node state changes to SYNCHRONIZED, the command:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED

1 instance(s)
```

Results

User understands the possible root causes of a node failing to synchronize with ENM the first time.

3.4 Unsupported MINI-LINK Indoor Node Version (Treat-as Functionality)

If the specific node version is not supported by ENM, the node will be managed in Treat-as mode. For additional information on Treat-as, refer to the *Configuration Management Overview* in the page 296.

This section provides information on steps to identify and troubleshoot Treat-as issues during Synchronization of a MINI-LINK-Indoor node.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Run the command below in ENM CLI to obtain a list of supported `ossModelIdentities`:

```
cmedit describe --netype <NE Type>
```

For example, to check supported versions of MINI-LINK Indoor nodes and corresponding `ossModelIdentity`:

```
cmedit describe -netype MINI-LINK-Indoor

Ne Type : MINI-LINK-Indoor
Ne Release : 17A
Product Identity : CXP9010021
Revision (R-State) : R34G
Functional MIM Name : -
Functional MIM Version : -
Model ID : M17A-TN-6.0

...

5 instance(s)
```

There are three cases where `ossModelIdentity` may not be valid :

a. It is not set.

b. It is set to an unsupported or invalid version

2. To check the value of `ossModelIdentity` for a specific node, enter this command in ENM CLI:

```
cmedit get <NodeName> NetworkElement.ossModelIdentity
FDN : NetworkElement=<NodeName>
ossModelIdentity :<ossModelIdentityValue>

1 instance(s)
```

3. Optionally, to confirm that this issue is related to synchronizing an empty or unsupported `ossModelIdentity`, check the logs for the following:

Level	Log message(s)	Meaning	Actions
WARN	`No suitable model identity found for '<NE FDN>': <IDENTITY> <REVISION>`	No model in ENM is applicable for the network element. See *OSS Model Identities and revisions of MINI-LINK Indoor* in *ENM Supported Network Elements* for reference of supported product identities and revisions.	Set the `ossModelIdentity` attribute to a compatible value to synchronize the node in treat-as mode.
INFO	`Could not identify the node '<NE FDN>' based on the values <IDENTITY> : <REVISION>`	Version attributes read from the node don't match the standard conventions.	
WARN	`Can't synchronize '<NE FDN>' because the OSS model identity is not known.`	Software synchronization could not find a suitable `ossModelIdentity` and no model identity is configured as manual treat-as. NE version might be too old or not supported	

Example

ossModelIdentity not set

```
[root@ms-1]# for i in $(cat /etc/hosts | egrep "mssnmpcm\s" | awk '{print $2 →
}'); \
do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "No suitable model identity found for\|Could not identify the node\|be →
cause the OSS model identity is not known" \
/ericsson/3pp/jboss/standalone/log/server.log*'; done
```

```
Logging into svc-2-mssnmpcm
WARN  [com.ericsson.oss.mediation.cm.snmp.swsync.ModelIdentityMatcherBean] ( →
Thread-13 (HornetQ-client-global-threads-285621782)) No suitable model ident →
ity found for 'NetworkElement=ML_indoor_1': CXP9010021_1 R1A1
INFO  [com.ericsson.oss.mediation.minilink.indoor.cm.handler.SoftwareSynchro →
nizationHandler] (Thread-8 (HornetQ-client-global-threads-285621782)) Could  →
not identify the node 'NetworkElement=ML_indoor_2' based on the values CXP90 →
10021_1 : P1A1

[root@ms-1 ~]#
```

4. If the `ossModelIdentity` value is empty or invalid, set it with this command:

```
cmedit set <NodeName> NetworkElement ossModelIdentity=<ossModelIdentity>
FDN : NetworkElement=<NodeName>
1 instance(s) updated
```

5. To force the synchronization of the node, run a manual sync command:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 sync
FDN : NetworkElement=<NodeName>,CmFunction=1
1 instance(s)
```

6. It may take some time for the node to synchronize. Execute the below command until the node state changes to SYNCHRONIZED:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED
1 instance(s)
```

Results

User identifies and troubleshoot failures in synchronization scenarios due to "Treat-as" issues.

4 CM Node Synchronization Troubleshooting - Nodes Supporting ECIM

Note: Use mscmce troubleshooting steps in case of mscmapg troubleshooting also.

4.1 Troubleshoot Node Heartbeat

Use this procedure to determine if there are issues with the node heartbeat.

Prerequisites

— Basic knowledge of the usage of CM CLI

— Basic knowledge of Linux

Heartbeat Timestamp Troubleshooting

Steps

1. Enter the following command to get a timestamp value (changing every 3 minutes).

```
cmedit get NetworkElement=<node-name> CmNodeHeartbeatSupervision.heartbeatTim →
estamp
```

2. If no such value exists, check the node synchronization with the following command:

```
cmedit get <node-name> CmFunction.syncStatus
```

   If the node is `SYNCHRONIZED`, at the end of each heartbeat interval, the status `DELTA` should appear in the `syncStatus` field.

3. If the node is `UNSYNCHRONIZED`, check if the supervision is active with the following command:

```
 cmedit get <node-name> CmNodeHeartbeatSupervision.active
```

4. If the output of this command is `false`, the node supervision is not active. Activate it to receive heartbeat notifications.

5. If the output of this command is `true`, there may be errors in the node configuration. Check whether the node is configured correctly.

6. If the node is configured correctly, check if the netconf LONG LIFE session exists.

   If the LONG LIFE session exists and the node is correctly configured, the `HeartbeatTimestamp` should change every 3 minutes.

   Since it unknown which mscmce instance manage the node is referred to, access every instance of mscmce and run the following command from the `/opt/ericsson/jboss/modules/com/ericsson/oss/mediation/adapter/netconf/jca/scripts` directory:

   ```
   ./debugger.sh showNetconfSessionRegistry | grep <node-name> | grep LONG_LIFE
   ```

   If there are issues with the long life session, no lines are printed. The normal behavior is represented by one line with the node name, `CONNECTED` status and XAProvider equals to LONG LIFE.

7. Ensure that other information available are aligned with the information that can be obtained from Configuration Management Command Line Interface (CLI).

8. Verify that there are not two instances of the same node with different transport protocol (for example: SSH on one side and TLS on the other), or different IP address in the tables retrieved between all the mscmce instances. If that is the case execute the following steps:

   a. From CM CLI, disable CM supervision for the referred node.

      ```
      cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervision=1 a →
      ctive=false
      ```

   b. From LMS, restart in sequence each mscmce where <node-name> LONG LIFE exists.

      ```
      /opt/ericsson/enminst/bin/vcs.bsh --restart -g Grp_CS_svc_cluster_m →
      scmce -s <cluster-id>
      ```

   c. From CM CLI, enable CM supervision for the referred node.

      ```
      cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervision=1 a →
      ctive=true
      ```

9. If no instance with LONG LIFE session is found in the table, set the node supervision to `false` and then back to `true` with the following commands:

   ```
   cmedit set NetworkElement=<node-name>
                        ,CmNodeHeartbeatSupervision=1 active=false
   cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervision=1 active=tru →
   e
   ```

10. Alternatively, check that in the Session Info the entries are correct (if the node is configured correctly).

Since it unknown which mscmce instance manage the node is referred to, access every instance of mscmce and run the following command from the `/opt/ericsson/jboss/modules/com/ericsson/oss/mediation/adapter/netconf/jca/scripts` directory:

```
./debugger.sh showSessionsInfo | grep <node-name>
```

The result of this command must be a non-empty set.

Example 1 Example messages in the mscmce server.log file when the supervision is enabled on the node

Note: The variable values must be replaced with proper values based on the environment.

```
2016-10-27 11:28:34 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] NetworkElement=<node-name>,CmFunction=1,CmNodeHeartbeatSupervision=1 →
 is managed by running MS(svc-x-mscmce) with valid status true
2016-10-27 11:28:34 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): Check periodic sync successfully c →
ompleted for the node: NetworkElement=<node-name>,CmFunction=1
2016-10-27 11:28:34 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): Finished at >>VALIDATE HEARTBEAT A →
ND CHECK CREATE SUBSCRIPTION<< CM HEARTBEAT HANDLER with Operation Type PERIODIC →
.
```

Example 2 Example messages in the mscmce server.log file when the supervision is disabled on the node

Note: The variable values must be replaced with proper values based on the environment.

```
2016-10-27 11:28:34 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] NetworkElement=<node-name>,CmFunction=1,CmNodeHeartbeatSupervision=1 →
 is managed by running MS(svc-x-mscmce) with valid status true
2016-10-27 11:28:34 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] FDN:NetworkElement=<node-name>: PREPARE FOR NEXT STEP =>> FdnHeaderN →
ame:NetworkElement=<node-name>, OperationType:DELETE, HB_Interval:1800, HB_Timeout →
:10, NumberOfRetries:3, StartTime:null
```

Example 3 Examples of messages in the mscmce server.log file when, at the end of the periodic heartbeatInterval, the node is *<SYNCHRONIZED>* but the heartbeat timestamp is obsolete and a new sync is issued

Note: The variable values must be replaced with proper values based on the environment.

```
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] NetworkElement=<node-name>,CmFunction=1,CmNodeHeartbeatSupervision=1 →
 is managed by running MS(svc-x-mscmce) with valid status true
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): Check periodic sync successfully c →
ompleted for the node: NetworkElement=<node-name>,CmFunction=1
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): getHeartbeatStartTime: lastNotific →
ation is 2016-10-27T11:28:35Z.THIS IS STARTTIME
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] FDN:NetworkElement=<node-name>: PREPARE FOR NEXT STEP =>> FdnHeaderN →
```

```
ame:NetworkElement=<node-name>, OperationType:CREATE, HB_Interval:60, HB_Timeout:1 →
0, NumberOfRetries:901, StartTime:2016-10-27T11:28:35Z
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): Finished at >>HEARTBEAT TIMESTAMP →
IS INVALID<< CM HEARTBEAT HANDLER with Operation Type PERIODIC.
```

Example 4 Example of messages in the mscmce server.log file when, at the end of the periodic heartbeatInterval, the node is *<SYNCHRONIZED>* and no issue is found in the timestamp

Note: The variable values must be replaced with proper values based on the environment.

```
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): getHeartbeatStartTime: lastNotific →
ation is 2016-10-27T11:28:35Z. THIS IS STARTTIME
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] FDN:NetworkElement=<node-name>: PREPARE FOR NEXT STEP =>> FdnHeaderN →
ame:NetworkElement=<node-name>, OperationType:CREATE, HB_Interval:60, HB_Timeout:1 →
0, NumberOfRetries:901, StartTime:2016-10-27T11:28:35Z
2016-10-27 11:28:35 INFO [com.ericsson.oss.mediation.handlers.handler.EcimCmHear →
tbeatHandler] (FDN:NetworkElement=<node-name>): Finished at >>VALIDATE HEARTBEAT A →
ND CHECK CREATE SUBSCRIPTION<< CM HEARTBEAT HANDLER with Operation Type CREATE.
```

4.2 Troubleshoot Node Notifications

Use this procedure to verify that the node notifications are working correctly.

Prerequisites

— Basic knowledge of the usage of CM Command Line Interface (CLI)

— Basic knowledge of Linux

Node Notifications Troubleshooting

Steps

1. Check node synchronization with the following command:

   ```
   cmedit get <node-name> CmFunction.syncStatus
   ```

2. If the node results to be `UNSYNCHRONIZED`, notifications cannot be sent to ENM. Check if the supervision is active with the following command:

   ```
   cmedit get <node-name> CmNodeHeartbeatSupervision.active
   ```

3. If the output of this command is `false`, the node supervision is not active. Activate it to receive notifications.

4. If the output of this command is `true`, there may be errors in the node configuration. Check whether the node is configured correctly.

5. If the node is configured correctly, check if the channel to the node is established and active by checking the LONG LIFE session.

   Since it unknown which mscmce instance manage the node is referred to, access every instance of mscmce and run the following command from the `/opt/ericsson/jboss/modules/com/ericsson/oss/mediation/adapter/netconf/jca/scripts` directory:

   ```
   ./debugger.sh showNetconfSessionRegistry | grep <node-name> | grep LONG_LIFE
   ```

6. If there are issues with the long life session, no lines are printed. The normal behavior is represented by one line with the node name, `CONNECTED` status and XAProvider equals to LONG LIFE.

7. Ensure that other information available are aligned with the information that can be obtained from Configuration Management Command Line Interface (CLI).

   If the status is `CONNECTED` in the output, the channel and notifications are working correctly.

   If the status is `NOT CONNECTED`, it might be a connectivity issue (the node is not reachable or turned off). If there is a reconnect attempt every seven minutes check if the heartbeat is working correctly.

8. If no instance with LONG LIFE session is found in the table, set the node supervision to `false` and then back to `true` with the following commands:

   ```
   cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervision=1 active=fal →
   se
   cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervision=1 active=tru →
   e
   ```

4.3 Troubleshoot SGSN-MME Configuration

There is a limitation when managing the Serving GPRS Support Node (SGSN) and Mobility Management Entity (MME). The normal user id does not return a $ prompt on the SGSN-MME node, just ends with a #, for example, `=== om_admin@eqm01s14p2 ANCB ~ #`.

This results in Measurement Initiation and Administration (MIA) and Core Network Configuration Tasks (CNCT) script failure, because they expect a $ prompt.

Prerequisites

— Basic knowledge of Linux

— Root access of SGSN-MME node

4.3.1 Change Prompt on SGSN-MME

To change the prompt for the user, execute the appropriate step from the following:

Steps

1. Change Prompt of SGSN-MME using Root User

   There is a limitation when managing the SGSN-MME. The normal user id does not return a $ prompt on the SGSN-MME node. The prompt ends with a #, for example, === om_admin@eqm01s14p2 ANCB ~ #. This causes MIA and CNCT scripts to fail because they expect a $ prompt. To change the prompt for the user added above, do the following:

   ```
   Switch to root, do # su - root # passwd: ****** .
   Run usermod -s /bin/sh <newuser>.
   Switch to root, do # su - root # passwd: ******
   ```

   For Linux SGSN-MME (MkV, MkVI or later):

   Edit (or create if non-existent) the profile file (`/tmp/DPE_CORE/home/<user>/.profile`) for the newly added user by adding the following lines:

   ```
   PS1="$"
   TERM=vt100
   export PS1 TERM
   stty -echo
   stty -icanon
   PATH=/tmp/DPE_SC/LoadUnits/ttx/bin:$PATH
   export PATH
   ```

   Now when login occurs to the SGSN-MME node, prompt will be a $

2. Change Prompt of SGSN-MME (Removal of Root User)

   For node versions where root user is removed, om_admin user should be used to change the prompt.

   In this scenario, ssh <om_admin>@<node ip>

   Edit (or create if non-existent) the profile file (`/tmp/DPE_CORE/home/<user>/.profile`) for the newly added user by adding the following lines:

   ```
   PS1="$"
   TERM=vt100
   export PS1 TERM
   ```

```
stty -echo

sty -icanon

PATH = /tmp/DPE_SC/LoadUnits/ttx/bin:$PATH

export PATH
```

3. Change Prompt of SGSN-MME using external Ldap

   In case of external Ldap, tcsh shell should be used. Following is an example of user profile created in an external Ldap server

```
root@debian:/home/debian/ldapfiles# cat add_ userone_user.ldif
dn: uid= userone,ou=sgsnUsers,dc=sgsnexternal,dc=local
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
objectClass: pwdPolicy
pwdAttribute: userPassword
pwdPolicySubentry: cn=testPwdPolicy,ou=sgsnInternalData,dc=sgsnexternal,dc=l →
ocal
uid: userone
cn: userone
sn: userone
uidNumber: 10075
gidNumber: 802
homeDirectory: /home/userone
loginShell: /bin/sh
userPassword: {SSHA}msFUautEbtgk5xaRCfBtH5cUjvAQE6
```

4.4 Troubleshoot the Supervision of a Node

Use this procedure to ensure that the node is supervised so it can be synchronized with ENM.

Prerequisites

— Basic knowledge of the Configuration Management (CM) Command Line Interface (CLI).

Steps

1. If the CM supervision of the node is deactivated and a manual synchronization of the node is triggered in the CM CLI, the synchronization status of the node will be set to `UNSYNCHRONIZED` and an error is displayed shown in the Log Viewer.

   Example

```
ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (EJB default - 130) [ejbuser, COM →
_ECIM_SYNC_NODE.UPDATESYNCSTATUSHANDLER_ERROR, ALERT, Flow Engine, DPS Datab →
ase, Error in: com.ericsson.oss.mediation.cba.handlers.UpdateSyncStatusHandl →
er ('NetworkElement=<NodeName>,CmFunction=1'). Reset syncStatus to 'UNSYNCHR →
ONIZED'. Exception message: Synchronization request for this node has failed →
. Please ensure that the 'active' attribute in the 'CmNodeHeartbeatSupervisi →
on' ManagedObject has been set to true.]
```

2. Check the state of the node supervision with the following command:

```
cmedit get <NodeName> CmNodeHeartbeatSupervision.active
active : false

1 instance(s)
```

3. Activate the CM supervision for the node.

```
cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1 active=tru →
e
FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1

1 instance(s)
```

4. The supervision of the node is automatically triggered in ENM once the value of the `CmNodeHeartbeatSupervision.active` attribute changes from `false` to `true`.

   It may take a few minutes for the node to synchronize. Execute the following command until the node state changes to `SYNCHRONIZED`:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED

1 instance(s)
```

Results

The node is synchronized with ENM.

4.5 Troubleshoot Node Synchronization

Use this procedure to verify that the synchronization of nodes supporting ECIM are working correctly.

Prerequisites

— Basic knowledge of the CM Command Line Interface (CLI)

— Basic knowledge of Linux

— Node must be reachable from ENM

Enable log in case of sync failure

Steps

1. Log onto the mscmce VM and execute the following command:

```
> /ericsson/3pp/jboss/bin/jboss-cli.sh --connect
```

2. Enter the following commands to enable the debugging of the NETCONF:

```
/subsystem=logging/logger=com.ericsson.oss.mediation.netconf.handlers:add(le
vel=DEBUG)
/subsystem=logging/logger=com.ericsson.oss.mediation.util.netconf.parser:ad
d(level=DEBUG)
```

3. Enter the following command to enable the debugging of the synchronization:

```
/subsystem=logging/logger=com.ericsson.oss.mediation.cba.cm.handlers:add(lev
el=DEBUG)
```

4. Once complete, remove the handler using:

```
/subsystem=logging/logger=com.ericsson.oss.mediation.netconf.handlers:remove
/subsystem=logging/logger=com.ericsson.oss.mediation.util.netconf.parser:rem
ove
/subsystem=logging/logger=com.ericsson.oss.mediation.cba.cm.handlers:remove
```

5. Enter the following command to quit the Jboss CLI

```
quit
```

4.6 Router6000 Series Nodes, with LDAP User Enabled in ENM, Are Unsynchronized When Restored to a CV with No LDAP Configuration

An SHM job restores Router6000 nodes that have `ldapuser` enabled to a Configuration Version that has no `ldap` configuration. As a result, the nodes are left `UNSYNCHRONIZED`.

This problem can occur for Router6672, Router 6675, Router6x71, Router6273, and Router 6274 node types.

The following procedure fixes the problem.

Prerequisites

— The SSH protocol is used for communication between the node and ENM.

— The node configuration backup is secured without LDAP configuration.

Steps

1. Disable CM Supervision:

```
»cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1active=fal
se
```

2. Disable `LDAP User` for the node so that ENM does not use `ldapApplicationUse` for authentication purposes:

```
»secadm credentials update --ldapuser disable --nodelist <NodeName>
```

3. Enable CM Supervision:

```
»cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1active=tru →
e
```

4. Verify that the node is in `SYNCHRONIZED` status.

```
»cmedit get NetworkElement=<NodeName>,CmFunction=1
```

4.7 Unstable CM Node Synchronization for Router6000 Series Nodes

The CM Synchronization for Router6000 series nodes become unstable if managed in ENM with 500 or more nodes using SSH protocol.

For managing more than 500 Router6000 series nodes, it is recommended to use TLS rather than SSH.

Router6000 series nodes include Router6672, Router 6675, Router6x71, Router6273, and Router 6274 node types.

Steps on enrollment procedure to switch from SSH to TLS for Router6000 nodes is documented in CPI, for details see: *Online Certificate Enrollment on Router 6000 Family* in *Network Element Integration Configuration Overview Section* in ENM Operators Guide.

4.8 Troubleshoot NETCONF Bulk GET Response from COM or ECIM Node

Cause

The synch status of a node in ENM is UNSYNCHRONIZED if a node sends one of the following responses to the NETCONF bulk GET request:

— A partial response.

— A response that does not comply with the XML specification.

This troubleshooting task can only be completed if the node is reachable from the instance of the ENM `lvsrouter`.

There are separate procedures for nodes that support the SSH protocol and for nodes that support the TLS protocol..

Troubleshoot NETCONF Bulk GET Response from COM or ECIM Node That Supports the SSH Protocol

Note: To know the protocol and port of a node, refer to the section *Add a Node* in the online help for the Command Line Interface application.

Do the following steps to validate the response to ENM NETCONF bulk `GET` request in cases where the node supports the SSH protocol.

1. Log on to any `mscmce` instance of an ENM server and connect to a node on NETCONF interface.
2. Run the following command:

   ```
   ssh <node_username>@<node_ip> -p <ssh_port> -t -s netconf
   ```

   After you enter a password, the node lists the capabilities that it supports.
3. Share the following ENM capabilities with the node.

```
<?xml version="1.0" encoding="UTF-8"?>
 <hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <capabilities>
                <capability>urn:ietf:params:netconf:base:1.0</capability>
                <capability>urn:ietf:params:netconf:capability:notification:
1.0</capability>
                <capability>urn:ietf:params:netconf:capability:candidate:1.0
</capability>
                <capability>urn:ietf:params:netconf:capability:validate:1.0<
/capability>
                <capability>urn:ietf:params:netconf:capability:action:1.0</c
apability>
                <capability>urn:ietf:params:netconf:capability:rollback-on-e
rror:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capabil
ity>
                <capability>urn:ietf:params:xml:ns:netconf:capability:rollba
ck-on-error:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:writab
le-running:1.0</capability>
                <capability>urn:ietf:params:netconf:capability:writable-runn
ing:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:candid
ate:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:valida
te:1.0</capability>
                <capability>urn:ericsson:com:netconf:notification:1.1</capab
ility>
                <capability>urn:ericsson:com:sgsnmme:heartbeat:1.0</capabili
ty>
                <capability>http://www.ericsson.com/gsn/4.0/contentVersion</
capability>
                <capability>http://www.ericsson.com/gsn/3.0/protocolVersion<
/capability>
                <capability>urn:ericsson:com:netconf:action:1.0</capability>
                <capability>urn:ericsson:com:netconf:heartbeat:1.0</capabili
ty>
                <capability>urn:com:ericsson:ebase:1.1.0</capability>
                <capability>urn:com:ericsson:ebase:1.2.0</capability>
                <capability>urn:com:ericsson:ipos:exec-cli:1.0</capability>
                <capability>urn:com:ericsson:ipos:invoke-cli:1.0</capability
>
```

```
        </capabilities>
</hello>]]>]]>
```

4. Send the following NETCONF bulk **GET** request to the node.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="1" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get/>
</rpc>
]]>]]>
```

   The response includes the entire node MO hierarchy.

   Any incomplete termination of NETCONF bulk **GET** request is indicated by a Standard Error message, which indicates an issue from the node end.

Troubleshoot NETCONF Bulk GET Response from COM or ECIM Node That Supports the TLS Protocol

Note: To know the protocol and port of a node, refer to the section *Add a Node* in the online help for the Command Line Interface application.

Do the following steps to validate the response to ENM NETCONF bulk `GET` request in cases where the node supports the TLS protocol..

1. Log on to any `mscmce` instance of an ENM server and connect to a node on NETCONF interface.
2. Run the following command.

```
# openssl s_client -connect <node_ip>:6513 -cert tlsnetconf.cert -key tlsnet →
conf.key -CAfile tlsnetconfCA.pem
```

   When the connection is successful, the node lists the capabilities that it supports.

   — Example IPv4 Copmmand

```
# openssl s_client -connect 10.154.168.209:6513 -cert tlsnetconf.cert - →
key tlsnetconf.key -CAfile tlsnetconfCA.pem
```

   — Example: IPv6 Command

```
# openssl s_client -connect [2001:1b70:82a1:103::64:631]:6513 -cert tls →
netconf.cert -key tlsnetconf.key -CAfile tlsnetconfCA.pem
```

3. Check if the supplied `tlsnetconfCA.pem` file does not have the full certificate chain.

   This is the case if:

   — The `openssl` command fails with message `alert unknown ca`

— The node does not return its capabilities.

4. If the supplied `tlsnetconfCA.pem` file does not have the full certificate chain, add the missing certificates to the file.

    a. Create a copy of `tlsnetconfCA.pem` and `tlsnetconf.cert` in the `/var/temp` directory.

    ```
    # cp tlsnetconfCA.pem /var/tmp/tlsnetconfCA_new.pem
     # cp tlsnetconf.cert /var/tmp/tlsnetconf_new.cert
    ```

    b. Open the `/var/tmp/tlsnetconf_new.cert` file using the vi editor.

    This file consists of multiple certificates. Each certificate is enclosed between `BEGIN CERTIFICATE` and `END CERTIFICATE`.

    c. Create a copy of `tlsnetconfCA.pem` and `tlsnetconf.cert` in the `/var/temp` directory.

    d. Use any decoder tool to identify which certificate in the `/var/tmp/tlsnetconf_new.cert` file corresponds to `ENM_OAM_CA.crt` and `ENM_Infrastructure_CA.crt`.

    Note: The following is one way to extract each certificate from the `/var/tmp/tlsnetconf_new.cert` file that contains multiple certificates.

        i. Copy each certificate and save its contents in the `/var/tmp` directory. Use the following naming convention: `first.crt`, `second.crt`, and so on.

        ii. Execute the following command against each saved *<.crt>* file to identify which certificate the saved file contains.

        ```
        openssl x509 -in first.crt -text -noout | grep "Subjec
        t: CN"
        ```

        The output is similar to the following:

        ```
        Subject: CN=ENM_OAM_CA, OU=BUCI_DUAC_NAM, O=ERICSSON,
        C=SE
        ```

        iii. Check if the output contains the string `CN=`. If it does, rename the file from its current name (`first.crt`, `second.crt`, and so on) to whatever text appears after `CN=` (for example `ENM_OAM_CA.crt`).The two required certificates are `ENM_OAM_CA.crt` and `ENM_Infrastructure_CA.crt`.

    e. Open the `/var/tmp/tlsnetconfCA_new.pem` file. Append the `ENM_OAM_CA.crt` and `ENM_Infrastructure_CA.crt` certificates identified in the previous step to the end of the file. Save the file

f. Run the `openssl` command again with the `/var/tmp/tlsnetconfCA_new.pem` file.

```
openssl s_client -connect <node_ip>:6513 -cert tlsnetconf.cert -key
 tlsnetconf.key -CAfile /var/tmp/tlsnetconfCA_new.pem
```

5. Share the following ENM capabilities with the node.

```
<?xml version="1.0" encoding="UTF-8"?>
 <hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <capabilities>
                <capability>urn:ietf:params:netconf:base:1.0</capability>
                <capability>urn:ietf:params:netconf:capability:notification:
1.0</capability>
                <capability>urn:ietf:params:netconf:capability:candidate:1.0
</capability>
                <capability>urn:ietf:params:netconf:capability:validate:1.0<
/capability>
                <capability>urn:ietf:params:netconf:capability:action:1.0</c
apability>
                <capability>urn:ietf:params:netconf:capability:rollback-on-e
rror:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:base:1.0</capabil
ity>
                <capability>urn:ietf:params:xml:ns:netconf:capability:rollba
ck-on-error:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:writab
le-running:1.0</capability>
                <capability>urn:ietf:params:netconf:capability:writable-runn
ing:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:candid
ate:1.0</capability>
                <capability>urn:ietf:params:xml:ns:netconf:capability:valida
te:1.0</capability>
                <capability>urn:ericsson:com:netconf:notification:1.1</capab
ility>
                <capability>urn:ericsson:com:sgsnmme:heartbeat:1.0</capabili
ty>
                <capability>http://www.ericsson.com/gsn/4.0/contentVersion</
capability>
                <capability>http://www.ericsson.com/gsn/3.0/protocolVersion<
/capability>
                <capability>urn:ericsson:com:netconf:action:1.0</capability>
                <capability>urn:ericsson:com:netconf:heartbeat:1.0</capabili
ty>
                <capability>urn:com:ericsson:ebase:1.1.0</capability>
                <capability>urn:com:ericsson:ebase:1.2.0</capability>
                <capability>urn:com:ericsson:ipos:exec-cli:1.0</capability>
                <capability>urn:com:ericsson:ipos:invoke-cli:1.0</capability
>
        </capabilities>
</hello>]]>]]>
```

6. Send the following NETCONF bulk **GET** request to the node.

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="1" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
        <get/>
</rpc>
]]>]]>
```

The response includes the entire node MO hierarchy.

Any incomplete termination of NETCONF bulk **GET** request is indicated by a Standard Error message, which indicates an issue from the node end.

4.9 Troubleshoot an Unexpected ossPrefix of a COM/ECIM Node

A Distinguished Name (DN) Prefix (`dnPrefix`) provides the naming context allowing Network Elements (NE's) to be partitioned into logical domains. When a node is added to ENM, the `ossPrefix` that is set must match the `dnPrefix` set on the node (if the value is different to null). This task describes how to troubleshoot when an unexpected `ossPrefix` value is set on a node.

Note: For a COM/ECIM node the `DNprefix` can be a null value, but if the `DNprefix` is present, it must match the `OSSPrefix` value of ENM. The behavior is different from CPP nodes because for COM/ECIM nodes the value of ManagedElementId can be different than 1.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the CM CLI.

Steps

1. If the prefix of the node does not match the `ossPrefix` value set on `NetworkElement` MO, synchronization status is set to `UNSYNCHRONIZED`. To retrieve the `ossPrefix` and the synchronization status of the node, execute the following commands from the CM CLI.

```
1)    cmedit get <NodeName> NetworkElement.ossPrefix
    FDN : NetworkElement=<NodeName>
    ossPrefix : SubNetwork=LTE64,MeContext=<NodeName>

    1 instance(s)

2)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. Log on the management server and check all MSCMCE (Mediation Service Configuration Management for COM/ECIM) JBOSS logs as shown in the following.

   The error message is only seen on the MSCMCE instance that was attempting to synchronize the invalid node. The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in page 296.

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mscmce\s" | awk '{print $2 →
}'); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "ossPrefix set on ENM is different from dnPrefix set on the node" \
```

```
/ericsson/3pp/jboss/standalone/log/server.log* | grep <NodeName>'; done
Logging into svc-2-mscmce
2016-02-21 11:08:08,066 ERROR [com.ericsson.oss.mediation.service.MediationS →
erviceClientBean] \
(Thread-170 (HornetQ-client-global-threads-1985727431)) \
2016-02-21 11:09:08,066 ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (Camel (c →
ba-vertical-camel-context) thread #1 - JmsConsumer[ComEcimMdbNotificationLis →
tener_0]) [NO USER DATA, COM_ECIM_NOTIFICATIONS.COMECIMNOTIFDPSINVOKEHANDLER →
_ERROR, ALERT, Flow Engine, DPS Database, Error in: com.ericsson.oss.mediati →
on.handlers.ComEcimNotifDpsInvokeHandler ('NetworkElement=SGSN11'). '. Excep →
tion message: CE_NTF - DN[NetworkElement=SGSN11] SeqNum 881 SessionId 1 : FO →
RCE UNSYNC! ossPrefix set on ENM is different from dnPrefix set on the node. →
 Error in CREATE MO!!!!]
[root@ms-1 ~]#
```

3. The shown error message means that this node is managed by more than one network management system which implies that the node's `ossPrefix` can be over written resulting in synchronization failures.

4. To overcome the issue, it is necessary to manually set the `DNPrefix` value on the node and match it with the `OSSPrefix` of ENM or set it again as an empty string.

Results

When an unexpected `ossPrefix` is identified the cause of the synchronization fault is known.

4.10 Unsupported Node Version COM/ECIM (Treat-As Functionality)

If the specific node version is not supported by ENM, the node will be managed in Treat-as mode. For additional information on Treat-as, refer to the *Configuration Management Overview* in the page 296.

This section provides information on steps to identify and troubleshoot Treat-as issues during Synchronization of a node.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Run the command below in ENM CLI to obtain a list of supported `ossModelIdentities`:

```
cmedit describe --netype <NE Type>
```

For example, to check supported versions of SGSN nodes and corresponding `ossModelIdentity`:

```
cmedit describe --netype SGSN

Expected Output :

Ne Type | Ne Release | Product Identity | Revision (R-State) | Functional MI →
M Name | Functional MIM Version |     Model ID
SGSN-MME           -              -                  -              Sgsn  →
               1.5.1                    16A_CP12
SGSN-MME           -              -                  -              Mme   →
             1.5.1                    16A-CP12
SGSN-MME           -              -                  -              Sgsn  →
               1.4.1                    16A-CP06
SGSN-MME           -              -                  -              Mme   →
               1.4.1                    16A-CP06
```

There are three cases where `ossModelIdentity` is not valid :

a. It is not set.

b. It is set to an unsupported or invalid version

c. It is set to a non backwards compatible version

Results

User identifies and troubleshoot failures in synchronization scenarios due to "Treat-as" issues.

4.10.1 Unsupported Node Version COM/ECIM (Treat-As Functionality): Case B

Note: For case b, note that ENM model identity identifies a combination of the models supported by the node. In particular, for COM/ECIM nodes it identifies the MIM version plus the PmEvent model. So the model identity of a COM/ECIM node including a MIM version supported in ENM can result unsupported if the version of PM model is different from the one included in the model version supported by ENM. In this case as the OSS model identity cannot be automatically set during the software synchronization, it must be set by the operator as in treat-as scenario.

Steps

1. To check the value of `ossModelIdentity` for a specific node, enter this command in ENM CLI:

```
cmedit get <NodeName> NetworkElement.ossModelIdentity
FDN : NetworkElement=<NodeName> ossModelIdentity :<ossModelIdentityValue>
1 instance(s)
```

2. Optionally, to confirm that this issue is related to synchronizing an empty or unsupported `ossModelIdentity`, log on to the ENM MS as a **`litp-admin`** user, switch to the root user, and check all Mediation Service for

Configuration Management for ECIM nodes (MSCME) JBOSS logs using the following commands.

The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in the page 296.

`ossModelIdentity` not set

```
[root@cloud-ms-1~]# for i in $(cat /etc/hosts | egrep "mscmce\s" | awk '{pri →
nt $2}');
do echo "Logging into ${i}"; ssh -i /root/.ssh/vm_private_key cloud-user@${i →
}
'grep "Set NetworkElement with valid value of OSSModelIdentity." \
/ericsson/3pp/jboss/standalone/log/server.log* | \
grep "COM_ECIM_SYNC_NODE.TREATASHANDLER_ERROR" | \
grep "NetworkElement=<NodeName>" '; done


Logging
into svc-1-mscmce
ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (Thread-107 (HornetQ-client-globa →
l-threads-222486848)) [NO USER DATA, COM_ECIM_SYNC_NODE.TREATASHANDLER_ERROR →
, ALERT, Flow Engine, DPS Database,
 Error in: com.ericsson.oss.mediation.cba.handlers.TreatasHandler ('NetworkE →
lement=SGSN-16A-CP03-V101,CmFunction=1'). Reset syncStatus to'UNSYNCHRONIZED →
'. Exception message: OssModelIdentity: [] not supported by
model service for neType: SGSN-MME. For Treat-as Sync, Set NetworkElement wi →
th valid value of OSSModelIdentity.]
```

unsupported `ossModelIdentity`

```
[root@cloud-ms-1
~]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}');
do echo "Logging into ${i}"; ssh -i /root/.ssh/vm_private_key
cloud-user@${i} 'grep "ossModelIdentity is invalid or not supported." \
/ericsson/3pp/jboss/standalone/log/server.log* \
| grep "ERROR" | grep "OssModelIdentityHandler" '; done


Logging
into svc-1-mscm
ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (EJB default - 220) [ejbuser, Oss →
ModelIdentityHandler_ERROR, ERROR, Live View,NetworkElement=SGSN-16A-CP03-V1 →
01, ossModelIdentity is invalid or not
supported. Use 'cmedit describe -neType SGSN-MME' to obtain a list of validM →
odel IDs for this neType. The ossModelIdentity is only mandatory in Treat-As →
 mode.]
```

3. If the `ossModelIdentity` value is invalid, set it with this command:

```
cmedit set <NodeName> NetworkElement ossModelIdentity=<ossModelIdentity>
FDN : NetworkElement=<NodeName>
1 instance(s) updated
```

4. To force the synchronization of the node, run a manual sync command:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 sync
FDN : NetworkElement=<NodeName>,CmFunction=1
1 instance(s)
```

5. It may take some time for the node to synchronize. Execute the below command until the node state changes to SYNCHRONIZED:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED
1 instance(s)
```

4.11 Troubleshoot BSC Synch Failures

> Scenarios for troubleshooting BSC synch failures are described here. The troubleshooting requires a knowledge of the CM CLI.

Cause 1: A Sync (Read) Operation Is Performed during the `DELETE MO` Operation, Resulting in `CM SYNCH` Issues and Data-Conversion Errors in ENM

Only supervised nodes can be synchronized with ENM. Typically, DB data is not locked during data read operations between COM and the BSC database. The following error is returned in this use case:

```
2019-02-15 12:06:27,469 ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (Thread-1196 (HornetQ-client-gl →
obal-threads-379250589)) [NO USER DATA, COM_ECIM_SYNC_NODE.MANAGEDOBJECTHANDLER_ERROR, WARNING, Fl →
ow Engine, DPS Database, Data conversion exception for networkElement:NetworkElement=BSC115, estim →
atedFdn:ManagedElement=1,BscFunction=1,BscM=1,GeranCellM=1,GeranCell=807. Continue transforming :M →
anagedObject- GeranCell807 key attribute-geranCellId is null or empty]
```

Solution

Typically the inconsistencies are resolved automatically in the coming heartbeat cycles. The resolution occurs after the completion of corresponding DELETE operations on the node.

If any inconsistency remains, perform manual sync for the node, as shown here:

```
cmedit action NetworkElement=XXXXXX,CmFunction=1
```

The BSC node is synchronized to ENM.

Cause 2: Incorrect Node Configuration Triggers NETCONF Response Containing a NULL or EMPTY Value for the <MO Name> Id Attribute of Any MO That Presents on BSC Node Configuration

In this scenario, the parsing for the NETCONF response fails in ENM, causing the BSC node to have a status of CM Unsynchronized. The following is the sample ERROR message that is visible in one of the following locations:

— Log viewer

— The `mscmapg` VM `server.log` file

```
ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (Thread-398 (HornetQ-client-global-threads-1384480197))
 [NO USER DATA, COM_ECIM_SYNC_NODE.FINALIZESYNCHANDLER_ERROR, ALERT, Flow Engine, DPS Database, Er
ror in: FinalizeSyncHandler ("NetworkElement=BSCENC2,CmFunction=1"). Reset syncStatus to "UNSYNCHR
ONIZED". Exception message: Sync is failed due to Data-Conversion errors, found in 3 managedObejec
ts.]
```

Solution

1. Identify every MO presenting on the BSC node that returned the error.
2. Give each identified MO a correct id attribute.

   The BSC node is synchronized to ENM.

Cause 3: Incorrect Node Configuration Triggers a NETCONF Response Containing Invalid (JUNK) Value

In this scenario, the parsing for the NETCONF response fails in ENM, causing the BSC node to have a status of CM Unsynchronized. The following is the sample ERROR message that is visible in one of the following locations:

— Log viewer

— The `mscmapg` VM `server.log` file

```
2019-08-02 19:40:58,348 ERROR [com.ericsson.oss.mediation.util.netconf.parser.NetconfStreamParser]
 (Thread-31 (HornetQ-client-global-threads-2026111873)) Exception trying to parse the rpc-reply re
ceived from the node.: org.xml.sax.SAXParseException; lineNumber: 61552; columnNumber: 52; Invalid
 byte 1 of 1-byte UTF-8 sequence.
```

Solution

1. Identify every MO presenting on the BSC node that returned the error.
2. Give each identified MO a correct id attribute.

   The BSC node is synchronized to ENM.

4.11.1 Blacklist BSC FileM Mo

> This section provides the detailed workaround for blacklisting the FileM Mo.

The DriverQueryExecutionException can occur when the operator tries to sync large BSC nodes and the node gets unsynced after particular time period.

```
com.ericsson.oss.itpf.datalayer.dps.neo4j.driver.client.api.exce →
ption.DriverQueryExecutionException: Failed to invoke procedure  →
`ericsson.driver.persist`: Caused by: org.neo4j.internal.kernel. →
api.exceptions.EntityNotFoundException: Unable to load RELATIONS →
HIP with id 974967
```

To sync the node, do the following:

Steps

1. Disable supervision, delete NRM data

   ```
   cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
   ion=1 active=false

   cmedit set NetworkElement=<Node Name>,InventorySupervision=1  →
   active=false

   cmedit set NetworkElement=<Node Name>,PmFunction=1 pmEnabled= →
   false

   alarm disable <Node Name>

   cmedit action NetworkElement=<Node Name>,CmFunction=1 deleteN →
   rmDataFromEnm
   ```

   Note: Delete the data from DPS directly by dps-data-fixer-tool. if any error occurs while deleting NRM data. See Remove an Attribute on a given MO on page 34

2. Apply FileM blacklist

   — Log on to any mscmapg SG as root.

   — Create directory `/ericsson/tor/data/mscmapg`.

   — Create CSV files based on node type in the created directory. CSV filename must be the node type.

   For example, BSC.csv content as:

   ```
   ossModelIdentity:mo:ns:excludeCompleteMo:attr:excludeFrom →
   Sync

   1185-481-418:FileM:ComFileM:true::true
   ```

   Note: Whenever the node OMI is changed, change the BSC.csv and update accordingly.

— Update the PIB parameter blackListPath to `ericsson/tor/data/mscmapg`.

```
[cloud-user@svc-X-mscmapg ~]$sudo /opt/ericsson/
PlatformIntegrationBridge/etc/config.py update --
app_server_address=<mscmapg-instance>:8080 --
name=blackListPath --value=/ericsson/tor/data/mscmapg
```

— Read the value and ensure it is the same.

```
[cloud-user@svc-X-mscmapg ~]$sudo /opt/ericsson/
PlatformIntegrationBridge/etc/config.py read --
app_server_address=<mscmapg-instance>:8080 --
name=blackListPath
```

3. Increase HB life cycle time to allow initial syncing of large BSC (BSC having Mo's > 500k).

```
cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
ion=1 heartbeatInterval = 1800
```

Read the value after setting and it must show 1800.

4. Enable Supervision and wait for the node sync.

```
cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
ion=1 active=true

cmedit set NetworkElement=<Node Name>,InventorySupervision=1 →
active=true

cmedit set NetworkElement=<Node Name>,PmFunction=1 pmEnabled= →
true

alarm enable <Node Name>
```

5. Revert HB lifecycle time changes done in Step 3.

```
cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
ion=1 heartbeatInterval = 420
```

4.11.1.1 Remove an Attribute on a given MO

Prerequisites

— If the ENM ISO version is older than 1.91.95:

- Ensure to download the latest dps-data-fixer-tool.

- It must be installed in a temporary folder in one of the db blades.
- It must be executed by user root.

— If the ENM ISO version is 1.91.95 or later:

- The tool is on a db node under the directory: `/opt/ericsson/neo4j/dps/dps-data-fixer/`.
- Go to the directory and continue from Step 6.

Steps

1. Log on to the db blade host where the latest dps-data-fixer-tool is downloaded.

   ```
   [root@LMS:~]#ssh litp-admin@ <db node name>
   ```

2. Switch user to root.

   ```
   [litp-admin@db-1:~]$su -
   ```

3. Change to temporary folder.

   ```
   [root@db-1]#cd /var/tmp
   ```

4. Extract the downloaded tool.

   ```
   [root@db-1:tmp]#unzip 19089-CXP9032728_X_G_TAR_GZIPV1.tar.gz

   [root@db-1:tmp]#cd dps-data-fixer
   ```

5. Ensure binary java is accessible through Linux PATH.

   ```
   [root@db-1:dps-data-fixer]#type java

   java is /usr/bin/java

   [root@db-1:dps-data-fixer]#echo $PATH

   /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/
   bin:/opt/ericsson/enmutils/bin:/opt/ericsson/enminst/bin:/
   root/rvb/bin:/root/bin
   ```

6. Run the following command:

   Note: All values must be escaped with single quotes.

   a. dps-data-fixer.sh -fix REMOVE_ATTRIBUTE -moFdn '<FDN>' -attribute '<attribute Name>' -batchSize '<size>'

      Note: The batch size must not be greater than 10,000.

```
./dps-data-fixer/dps-data-fixer.sh -fix REMOVE_ATTRIBUTE
-moFdn 'SubNetwork=ONRM_ROOT_MO,SubNetwork=NIC_AXE,MeCont
ext=BSCSE2H,ManagedElement=BSCSE2H,SystemFunctions=1,File
M=1,LogicalFs=1,FileGroup=data_transfer,FileGroup=destina
tions,FileGroup=OSSCHECK,FileGroup=Ready' -attribute 'fil
es' -batchSize '5000'
```

b. The command reports the attribute to be removed from the given MO. A similar output can be observed as follows:

Note: If the attribute to be removed is a large list of CDTs, the tool can take a long time to retrieve the required data from the DB. (A list that contains over 121K CDTs, the tool can take over 10 minutes to finish.)

```
[root@db-1 ~]#./dps-data-fixer/dps-data-fixer.sh -fix
REMOVE_ATTRIBUTE -moFdn
'SubNetwork=ONRM_ROOT_MO,SubNetwork=NIC_AXE,MeContext=BSCS
E2H,ManagedElement=BSCSE2H,SystemFunctions=1,FileM=1,Logic
alFs=1,FileGroup=data_transfer,FileGroup=destinations,File
Group=OSSCHECK,FileGroup=Ready' -attribute 'files' -
batchSize '5000'
```

```
Dps_Data_Fixer: [INFO] Validating script requirements.
Dps_Data_Fixer: [INFO] Running script on a Physical deplo
yment.
Dps_Data_Fixer: [INFO] Retrieving neo4j credentials on ph
ysical.
Dps_Data_Fixer: [INFO] Running script on a Physical deplo
yment.
Dps_Data_Fixer: [INFO] Will execute job on host: neo4j3
Dps_Data_Fixer: [INFO] Neo4j is running in cluster mode
Dps_Data_Fixer: [INFO] Not Setting any max heap size
Dps_Data_Fixer: [INFO] Calling data fixer with arguments
:  -host 10.247.246.7 -port 7687 -cluster false -user neo
4j -pw ********** -fix REMOVE_ATTRIBUTE -moFdn SubNetwork
=ONRM_ROOT_MO,SubNetwork=NIC_AXE,MeContext=BSCSE2H,Manage
dElement=BSCSE2H,SystemFunctions=1,FileM=1,LogicalFs=1,Fi
leGroup=data_transfer,FileGroup=destinations,FileGroup=OS
SCHECK,FileGroup=Ready -attribute files -batchSize 5000
2020-04-16 10:32:23 INFO  [main] RemoveAttributeFixer - G
etting AttributeStatus
Apr 16, 2020 10:32:23 AM org.neo4j.driver.internal.loggin
g.JULogger info
INFO: Direct driver instance 1518864111 created for serve
r address 10.247.246.7:7687
2020-04-16 10:32:24 INFO  [main] RemoveAttributeFixer - M
O attribute keys: [ _s:files,  _level,  _name,  _namespac
e,  _bucket,  _version,  _internalId,  _createdTime,  _bu
cketFdn, fileGroupId,  _type,  _lastUpdatedTime,  _isMibR
oot,  _fdn]
```

```
2020-04-16 10:32:24 INFO  [main] RemoveAttributeFixer - A →
ttribute: files to be removed is of status: IS_LIST_OF_CD →
TS
2020-04-16 10:32:24 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24246101
2020-04-16 10:32:25 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24213995
2020-04-16 10:32:26 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24255100
2020-04-16 10:32:26 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24215911
2020-04-16 10:32:27 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24257283
2020-04-16 10:32:28 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24225937
2020-04-16 10:32:29 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24260994
2020-04-16 10:32:30 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24229451
2020-04-16 10:32:30 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24270179
2020-04-16 10:32:31 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24230457
2020-04-16 10:32:32 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24275162
2020-04-16 10:32:33 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24344686
2020-04-16 10:32:34 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24276883
2020-04-16 10:32:34 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24346554
2020-04-16 10:32:35 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24186266
2020-04-16 10:32:36 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24355958
2020-04-16 10:32:37 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24190949
2020-04-16 10:32:38 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24298467
2020-04-16 10:32:38 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24192890
2020-04-16 10:32:39 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24235233
2020-04-16 10:32:40 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24201098
2020-04-16 10:32:41 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24239195
2020-04-16 10:32:42 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24202899
2020-04-16 10:32:42 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24248460
2020-04-16 10:32:43 INFO  [main] RemoveAttributeFixer - R →
```

```
etrieving next ids batch, starts next to: 24212863
2020-04-16 10:32:43 INFO  [main] RemoveAttributeFixer - R →
etrieving next ids batch, starts next to: 24239826
2020-04-16 10:32:43 INFO  [main] RemoveAttributeFixer - D →
eleting 26 CDT batches
2020-04-16 10:32:43 INFO  [main] RemoveAttributeFixer - D →
eleting 1/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 2/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 3/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 4/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 5/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 6/26 batch
2020-04-16 10:32:44 INFO  [main] RemoveAttributeFixer - D →
eleting 7/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 8/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 9/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 10/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 11/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 12/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 13/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 14/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 15/26 batch
2020-04-16 10:32:45 INFO  [main] RemoveAttributeFixer - D →
eleting 16/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 17/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 18/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 19/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 20/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 21/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 22/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 23/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
```

```
eleting 24/26 batch
2020-04-16 10:32:46 INFO  [main] RemoveAttributeFixer - D →
eleting 25/26 batch
2020-04-16 10:32:47 INFO  [main] RemoveAttributeFixer - D →
eleting 26/26 batch
2020-04-16 10:32:47 INFO  [main] RemoveAttributeFixer - R →
emoving  _s:files from MO: [Live::SubNetwork=ONRM_ROOT_MO →
,SubNetwork=NIC_AXE,MeContext=BSCSE2H,ManagedElement=BSCS →
E2H,SystemFunctions=1,FileM=1,LogicalFs=1,FileGroup=data_ →
transfer,FileGroup=destinations,FileGroup=OSSCHECK,FileGr →
oup=Ready]
2020-04-16 10:32:47 INFO  [main] RemoveAttributeFixer - A →
ttribute: files removed from MO[Live::SubNetwork=ONRM_ROO →
T_MO,SubNetwork=NIC_AXE,MeContext=BSCSE2H,ManagedElement= →
BSCSE2H,SystemFunctions=1,FileM=1,LogicalFs=1,FileGroup=d →
ata_transfer,FileGroup=destinations,FileGroup=OSSCHECK,Fi →
leGroup=Ready]
Apr 16, 2020 10:32:47 AM org.neo4j.driver.internal.loggin →
g.JULogger info
INFO: Closing driver instance 1518864111
Apr 16, 2020 10:32:47 AM org.neo4j.driver.internal.loggin →
g.JULogger info
INFO: Closing connection pool towards 10.247.246.7:7687
Dps_Data_Fixer: [INFO] Data fixer successfully executed.
```

c. Contact design team support in case of any difficulties while removing an attribute on a given MO.

4.11.2 Troubleshoot BSC CM

> Scenarios for troubleshooting BSC CM are described here.

Cause 1

Port and Protocol

Solution

Check if the ports, protocols, and IP Address of the node and child nodes are entered correctly.

Cause 2

There is chance of the node getting managed in one or more instances with duplicate connections because of protocol switch from SSH to TLS or conversely

while the CM supervision is still on. This results in multiple CM subscriptions for a node.

Solution

1. Disable the supervision on the node.
2. Restart all **mscmapg** instances at a time.
3. Enable the supervision on the node.

```
[cloud-user@svc-4-mscmapg log]$ /opt/ericsson/jboss/modules/c →
om/ericsson/oss/mediation/adapter/netconf/jca/scripts/debugge →
r.sh showConnectionsRegistry
dumpConnectionsRegistry operation executed:
================================================================ →
================================================================ →
=================
|| Connections Registry                                        →
                                                                →
              ||
================================================================ →
================================================================ →
=================
||  ServiceKey          | SubscriberKey  | Username       | I →
pAddress       | Port  | Protocol | Connected | Listener  | P →
eriodicTasks  ||
================================================================ →
================================================================ →
=================
||  cm_subscription     |                | ldapApplication| 1 →
0.78.13.166    | 830   | ssh      | false     | false     | 1 →
              ||
||  cm_subscription     |                |                     →
          | 10.78.13.166    | 6513  | tls      | false     |  →
false     | 1              ||
================================================================ →
================================================================ →
=================

[cloud-user@svc-2-mscmapg log]$
[cloud-user@svc-2-mscmapg log]$ /opt/ericsson/jboss/modules/c →
om/ericsson/oss/mediation/adapter/netconf/jca/scripts/debugge →
r.sh showConnectionsRegistry
dumpConnectionsRegistry operation executed:

================================================================ →
================================================================ →
=================
|| Connections Registry                                        →
                                                                →
```

```
              ||
============================================================ →
============================================================ →
=================
||  ServiceKey          | SubscriberKey  | Username       | I →
pAddress       | Port  | Protocol | Connected | Listener  | P →
eriodicTasks  ||
============================================================ →
============================================================ →
=================
||  cm_subscription     |                | netsim         | 1 →
0.152.200.145  | 22    | ssh      | true      | true      | 1 →
              ||
||  cm_subscription     |                | ts_bsc166      | 1 →
0.78.13.166    | 830   | ssh      | true      | true      | 1 →
              ||
============================================================ →
============================================================ →
=================
```

Cause 3

Node sync issue because of FileM Mo.

Solution

Refer Blacklist BSC FileM Mo on page 32 for detailed workaround.

Cause 4

If ENM is trying to perform some CRUD operations on some MO data on node which ideally does not exist on the node, it can cause RPC errors.

Solution

Check the issue mentioned in RPC error and look for the same on the node.

```
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" messa →
ge-id="1">
<rpc-error>
<error-type>rpc</error-type>
<error-tag>unknown-element</error-tag>
<error-severity>error</error-severity>
<error-info>
<bad-element>aggregationLevel</bad-element>
</error-info>
</rpc-error>
```

```
</rpc-reply>
]]>]]>
```

Cause 5

The current dimensioning for APG mediation supports synchronization up to 500K MOs for a GSM node. Check if the node has more than 500K MOs. If yes, then sync between node and ENM takes long time and sometimes resulting in the Heartbeat (HB) retries expiry. In this case, a parallel sync can get triggered because of which supervision gets toggled.

Multiple syncs are triggered in the following example:

```
2020-03-30 12:17:44,457 INFO [com.ericsson.oss.itpf.EVENT_DATA_L →
OGGER] (EJB default - 128) SyncStatusChange {"SyncStatus":"PENDI →
NG","_Thread":"EJB default - 128","Reason":"SW sync started","De →
tail":"","Node":"BSC183"}
2020-03-30 12:17:44,459 DEBUG [com.ericsson.oss.mediation.handle →
rs.common.SyncStatusUpdateHelper] (Thread-2929 (HornetQ-client-g →
lobal-threads-1054116001)) Current sync status for fdn NetworkEl →
ement=BSC183 is SYNCHRONIZED, Updating sync status to: PENDING

2020-03-30 12:17:59,790 DEBUG [com.ericsson.oss.mediation.handle →
rs.common.SyncStatusUpdateHelper] (Thread-2929 (HornetQ-client-g →
lobal-threads-1054116001)) Current sync status for fdn NetworkEl →
ement=BSC183 is PENDING, Updating sync status to: TOPOLOGY

2020-03-30 13:10:18,286 DEBUG [com.ericsson.oss.mediation.handle →
rs.common.SyncStatusUpdateHelper] (Thread-2996 (HornetQ-client-g →
lobal-threads-1054116001)) Current sync status for fdn NetworkEl →
ement=BSC183 is SYNCHRONIZED, Updating sync status to: PENDING

2020-03-30 13:17:46,409 ERROR [com.ericsson.oss.itpf.ERROR_LOGGE →
R] (Thread-3000 (HornetQ-client-global-threads-1054116001)) [NO  →
USER DATA, CM_HEARTBEAT_HANDLER.SYNC_ALREADY_IN_PROGRESS, WARNIN →
G, CM_HEARTBEAT_HANDLER, NetworkElement=BSC183, (FDN:NetworkElem →
ent=BSC183): A sync operation is already in progress for the nod →
e: 'NetworkElement=BSC183,CmFunction=1 too many times: force reS →
ubscribe with FullSync]
2020-03-30 13:17:46,409 WARN [com.ericsson.oss.mediation.handler →
s.handler.ComEcimCmHeartbeatHandler] (Thread-3000 (HornetQ-clien →
t-global-threads-1054116001)) (FDN:NetworkElement=BSC183): A syn →
c operation is already in progress for the node: 'NetworkElement →
=BSC183,CmFunction=1 too many times: force reSubscribe with Full →
Sync



2020-03-30 13:10:18,286 DEBUG [com.ericsson.oss.mediation.handle →
rs.common.SyncStatusUpdateHelper] (Thread-2996 (HornetQ-client-g →
```

```
lobal-threads-1054116001)) Current sync status for fdn NetworkEl →
ement=BSC183 is SYNCHRONIZED, Updating sync status to: PENDING
2020-03-30 13:10:34,159 DEBUG [com.ericsson.oss.mediation.handle →
rs.common.SyncStatusUpdateHelper] (Thread-2996 (HornetQ-client-g →
lobal-threads-1054116001)) Current sync status for fdn NetworkEl →
ement=BSC183 is PENDING, Updating sync status to: TOPOLOGY

2020-03-30 13:17:46,411 DEBUG [com.ericsson.oss.mediation.dps.Cm →
FunctionHelper] (Thread-3000 (HornetQ-client-global-threads-1054 →
116001)) HB updateSyncStatus - on MO NetworkElement=BSC183,CmFun →
ction=1 attribute syncStatus set to UNSYNCHRONIZED
2020-03-30 13:17:46,411 INFO [com.ericsson.oss.itpf.EVENT_DATA_L →
OGGER] (Thread-3000 (HornetQ-client-global-threads-1054116001))  →
SyncStatusChange {"SyncStatus":"UNSYNCHRONIZED","_Thread":"Threa →
d-3000 (HornetQ-client-global-threads-1054116001)","Reason":"CM  →
Heartbeat problem: Expired retries","Node":"NetworkElement=BSC18 →
3"}

[cloud-user@svc-4-mscmapg log]$ zgrep -a "SW sync started" serve →
r.log |grep BSC183
2020-03-31 13:19:27,499 INFO [com.ericsson.oss.itpf.EVENT_DATA_L →
OGGER] (EJB default - 212) SyncStatusChange {"SyncStatus":"PENDI →
NG","_Thread":"EJB default - 212","Reason":"SW sync started","De →
tail":"","Node":"BSC183"}
2020-03-31 13:21:29,401 INFO [com.ericsson.oss.itpf.EVENT_DATA_L →
OGGER] (EJB default - 98) SyncStatusChange {"SyncStatus":"PENDIN →
G","_Thread":"EJB default - 98","Reason":"SW sync started","Deta →
il":"","Node":"BSC183"}
2020-03-31 13:25:54,536 INFO [com.ericsson.oss.itpf.EVENT_DATA_L →
OGGER] (EJB default - 103) SyncStatusChange {"SyncStatus":"PENDI →
NG","_Thread":"EJB default - 103","Reason":"SW sync started","De →
tail":"","Node":"BSC183"}
```

Solution

1. Increase the HB time-out so that no parallel sync gets triggered.
2. Increase HB life cycle time to allow initial syncing of large BSCs (BSC having MOs greater than 500K).

   ```
   cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
   ion=1 heartbeatInterval = 1800
   ```

3. Read the value after setting. Result must show 1800.
4. Revert HB life cycle once the node is in sync state.

   ```
   cmedit set NetworkElement=<Node Name>,CmNodeHeartbeatSupervis →
   ion=1 heartbeatInterval = 420
   ```

Cause 6

CM sync failure because of **rpc-error** during bulk get response read occurs when COM component resources are not sufficient to do the job of reading data for multiple reasons. For this failure, some configuration changes are to be done on node end on COM side.

```
<rpc-error>
        <error-type>application</error-type>
        <error-tag>operation-failed</error-tag>
        <error-severity>error</error-severity>
        <error-message xml:lang="en">Request could not be perfor →
med - resource not available</error-message>
    </rpc-error>
```

Solution

No workaround from ENM, node side configuration to be corrected for COM.

Cause 7

CM sync failure to read **bulkget** response from node because of FileM data modified during read.

```
2020-07-08 12:48:18,613 ERROR [com.ericsson.oss.itpf.ERROR_LOGGE →
R] (Thread-15024 (HornetQ-client-global-threads-602451289))
[NO USER DATA, COM_ECIM_SYNC_NODE.NETCONFBULKGETHANDLER_ERROR, A →
LERT, Flow Engine, DPS Database,
Error in: com.ericsson.oss.mediation.cba.handlers.NetconfBulkGet →
Handler ('NetworkElement=BMO60D,CmFunction=1'). Reset syncStatus →
 to 'UNSYNCHRONIZED'.
Exception message: Error Type: applicationError Tag: RESOURCE_DE →
NIEDError Severity: errorError Message: no MO iterator available →
 for path: ManagedElement=BMO60D,SystemFunctions=1,FileM=1,Logic →
alFs=1,FileGroup=cp,FileGroup=printouts,FileGroup=adh,FileGroup= →
printouts, class name: FileGroup, error:ComTimeOut]
```

Solution

Retry the CM sync.

Whitelisting FileM does not solve the problem.

As FileM is modifying, wait and retry.

Cause 8

In lock or unlock operations, ENM receives CMSynchronization recommended notification from node and ENM triggers bulk sync operation. This causes delay in BSC node synchronization.

In this case, the number of MOs deleted on Node is high. So, deletion takes time in ENM. This is a special case where large MO tree is deleted on the node and KPIs defined for regular sync is not applied here.

Solution

This is a special case and BSC node synchronization takes time. However, with BSC: APG Mediation: Adapt Asynchronous Deletion of MO tree, there will be an improvement in performance.

Cause 9

In lock or unlock operations, ENM receives CMSynchronization recommended notification from node and ENM triggers bulk sync operation. In operations where MO count is greater than 500K BSC node synchronization fails.

In this case, the number of MOs deleted on Node is high. So, deletion fails as there is a limitation on number of changes in a single transaction in dps.

Solution

BSC: APG Mediation: Adapt Asynchronous Deletion of MO tree improvement fixes the issue of sync failures by using async dps api.

In sync failure, delete the NRM and then resync the node:

```
cmedit action NetworkElement=<node name>,CmFunction=1 deleteNrmD →
ataFromEnm
```

The following error is observed in logs in case of sync failure:

```
Caught exception mapped into XA Exception with Error Code: -3 - →
reason: Transaction is attempting to persist  {createdNodes=0,up →
datedNodes=1,deletedNodes=131177,createdRelationships=0,updatedR →
elationships=0,deletedRelationshipsIds=262354,createdProperties= →
0,updatedProperties=1,removedProperties=2889819} total no. of ch →
anges. Permissible limit is 1000000.
```

Cause 10

High CPU usage is observed on **mscmapg** VMs because of ssl renegotiation failure as ENM could not support it.

Solution

SSL renegotiation feature must be disabled in node side

4.12 Troubleshoot SNMP Security Settings for Node Synchronization After OAM IP Address Change

Use this procedure to verify that the synchronization of nodes after the OAM IP address change are working correctly.

Prerequisites

— Basic knowledge of the CM Command Line Interface (CLI).

— Node must be reachable from ENM.

Check the security settings of SnmpTargetV3=1 MO in ENM CLI are consistent with the values of parameter NODE_SNMP_SECURITY in ENM CLI.

Steps

1. Get the security settings of SnmpTargetV3=1 MO in ENM CLI:

   ```
   cmedit get SubNetwork=<subNetworkName>,ManagedElement=<nodeName>,SystemFunct →
   ions=1,SwM=1, Snmp=1,SnmpTargetV3=1
   ```

   Example

   ```
   cmedit get SubNetwork=LTE01dg2ERBS00001,ManagedElement=LTE01dg2ERBS00001,Sys →
   temFunctions=1,SysM=1,Snmp=1,SnmpTargetV3=1
   ```

2. Get the values of the `NODE_SNMP_SECURITY` parameter in ENM CLI:

   ```
   admin parameter view --name NODE_SNMP_SECURITY
   ```

3. If there is a mismatch in the values of step 1 and 2, manually update the security settings of SnmpTargetv3=1 MO with the corresponding values of the `NODE_SNMP_SECURITY` parameter.

5 CM Node Synchronization Troubleshooting - CPP Based Nodes

This section provides troubleshooting steps to diagnose common problems with node synchronization and notification handling of CPP based nodes.

5.1 Troubleshoot an Unexpected ossPrefix of a CPP Node

A Distinguished Name (DN) Prefix (`dnPrefix`) provides the naming context allowing Network Elements (NE's) to be partitioned into logical domains. When a node is added to ENM, the `ossPrefix` that is set must match the `dnPrefix` set on the node. This is necessary as the `dnPrefix` is needed to identify NE's uniquely in ENM as the node prepends this dnPrefix when sending data to ENM. This task describes how to troubleshoot when an unexpected `ossPrefix` value has been set on a node.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the CM CLI.

Steps

1. If the prefix of the node does not match the `ossPrefix` value set on `NetworkElement` MO, synchronization status will be set to `UNSYNCHRONIZED`. To retrieve the `ossPrefix` and the synchronization status of the node, execute the commands below from the CM CLI

```
1)    cmedit get <NodeName> NetworkElement.ossPrefix
    FDN : NetworkElement=<NodeName>
    ossPrefix : SubNetwork=LTE64,MeContext=<NodeName>

    1 instance(s)

2)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. Logon to the management server and check all MSCM (Mediation Service Configuration Management) JBOSS logs as shown below. The error message will only be seen on the MSCM instance that was attempting to synchronize the invalid node.

The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in the page 296.

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}' →
); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "Topology retreived from node does not contain expected DPS Root" \
/ericsson/3pp/jboss/standalone/log/server.log* | grep <NodeName>'; done
Logging into svc-2-mscm
2016-02-21 11:08:08,066 ERROR [com.ericsson.oss.mediation.service.MediationS →
erviceClientBean] \
(Thread-170 (HornetQ-client-global-threads-1985727431)) \
Exception occured possibly below mediation service in the stack (handlers, . →
..).
Node ID: [svc-2-mscm], request: [MediationTaskRequest [nodeAddress=NetworkEl →
ement=kienb1048,CmFunction=1, \
jobId=359fd68c-0475-4200-ac7c-5b6358dab923, protocolInfo=CM, clientType=EVEN →
T_BASED]], \
error: [javax.ejb.EJBException: org.jboss.camel.exception.CamelEngineRuntime →
Exception: \
Exception occurred: The topology retrieved from the node does not contain th →
e expected DPS Root \
FDN SubNetwork=ONRM_ROOT_MO_R,MeContext=kienb1048,ManagedElement=1. \
The mib prefix on the node seems to be incorrect.  \
The prefix on the node is set to: SubNetwork=ONRM_ROOT_MO_R,SubNetwork=LTEKi →
,MeContext=kienb1048,ManagedElement=1. \
This typically occurs when multiple management systems are managing the same →
 nodes.].\
2016-02-21 11:08:08,067 ERROR [org.jboss.as.ejb3.invocation] \
(Thread-170 (HornetQ-client-global-threads-1985727431)) JBAS014134: \
EJB Invocation failed on component MediationServiceClientBean for method \
public abstract void com.ericsson.oss.mediation.service.MediationServiceClie →
ntLocal.process\
(com.ericsson.oss.mediation.sdk.event.MediationTaskRequest): javax.ejb.EJBEx →
ception: \
com.ericsson.oss.mediation.service.MediationServiceException: \
Node ID: svc-2-mscm. org.jboss.camel.exception.CamelEngineRuntimeException:  →
\
Exception occurred: The topology retrieved from the node does not contain th →
e expected \
DPS Root FDN SubNetwork=ONRM_ROOT_MO_R,MeContext=kienb1048,ManagedElement=1. →
 \
The mib prefix on the node seems to be incorrect.  \
The prefix on the node is set to: SubNetwork=ONRM_ROOT_MO_R,SubNetwork=LTEKi →
,MeContext=kienb1048,ManagedElement=1. \
This typically occurs when multiple management systems are managing the same →
 nodes. \
Logging into svc-1-mscm
[root@ms-1 ~]#
```

3. The above error message means that this node is managed by more than one network management system which implies that the node's `ossPrefix` could be over written resulting in synchronization failures.

Results

When an unexpected `ossPrefix` is identified the cause of the synchronization fault is known

5.2 Unsupported Node Version (Treat-as Functionality)

If the specific node version is not supported by ENM, the node will be managed in Treat-as mode. For additional information on Treat-as, refer to the *Configuration Management Overview* in the page 296.

This section provides information on steps to identify and troubleshoot Treat-as issues during Synchronization of a node.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Run the command below in ENM CLI to obtain a list of supported `ossModelIdentities`:

   ```
   cmedit describe --netype <NE Type>
   ```

   For example, to check supported versions of ERBS nodes and corresponding `ossModelIdentity`:

   ```
   cmedit describe --netype ERBS

   Expected Output :

   Ne Type | Ne Release | Product Identity | Revision (R-State) | Functional MI →
   M Name | Functional MIM Version |     Model ID
   ERBS             -              -                  -               ERBS_NOD →
   E_MODEL             E.1.226            0828-946-594
   ERBS          -              -                  -              ERBS_NODE_M →
   ODEL             E.1.226          2870-147-123
   ERBS          -              -                  -               ERBS_NOD →
   E_MODEL             E.1.236            2414-850-363
   ERBS          -              -                  -               ERBS_NOD →
   E_MODEL             E.1.236            4053-309-342
   ```

   There are three cases where `ossModelIdentity` is not valid:

   a. It is not set.

   b. It is set to an unsupported or invalid version

   c. It is set to a non backwards compatible version

Results

User identifies and troubleshoot failures in synchronization scenarios due to "Treat-as" issues.

5.2.1 Unsupported Node Version (Treat-as Functionality): Case B

Note: For case b, note that ENM model identity identifies a combination of the models supported by the node. In particular, for CPP nodes it identifies the MIM version plus the `PmEvent` model. So the model identity of a CPP node including a MIM version supported in ENM can result unsupported if the version of PM model is different from the one included in the model version supported by ENM. In this case as the OSS model identity cannot be automatically set during the software synchronization, it must be set by the operator as in treat-as scenario.

Steps

1. To check the value of `ossModelIdentity` for a specific node, enter this command in ENM CLI:

```
cmedit get <NodeName> NetworkElement.ossModelIdentity
FDN : NetworkElement=<NodeName> ossModelIdentity :<ossModelIdentityValue>
1 instance(s)
```

2. Optionally, to confirm that this issue is related to synchronizing an empty or unsupported `ossModelIdentity`, log on to the ENM MS as the **`litp-admin`** user, switch to the root user, and check all Mediation Service for Configuration Management (MSCM) JBOSS logs using the following commands:

   The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in the page 296.

   `ossModelIdentity` not set

```
[root@ms-1]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}'); →
 \
do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "ossModelIdentity attribute needs to be set" \
/ericsson/3pp/jboss/standalone/log/server.log* | \
grep "SYNC_NODE.NODE_INFO_DPS_HANDLER_ERROR" | \
grep "NetworkElement=<NodeName>" '; done

Logging into svc-2-mscm
root@svc-2-mscm's password:
ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (Thread-71 (HornetQ-client-global →
-threads-1396894603)) [NO USER DATA, SYNC_NODE.NODE_INFO_DPS_HANDLER_ERROR,  →
ALERT, Flow Engine, DPS Database,
 Error in: NODE INFO DPS HANDLER ('NetworkElement=LTE01ERBS00004,CmFunction= →
1'). Reset syncStatus to 'UNSYNCHRONIZED'. Exception message: Could not sync →
hronize the node:
 NetworkElement=LTE01ERBS00004 as its version is not supported by ENM. The N →
etworkElement::ossModelIdentity attribute needs to be set, so that ENM knows →
 what version to treat the node as.
 See Online Help for Adding a Node and/or Describing Modelled Data for more  →
details on how to obtain a suitable value for this attribute]
Logging into svc-1-mscm
root@svc-1-mscm's password:
[root@ms-1 ~]#
```

   unsupported `ossModelIdentity`

```
[root@ms-1]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}'); →
 \
do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "No target version information exists for given target model identity" →
 \
/ericsson/3pp/jboss/standalone/log/server.log* \
| grep "ERROR" | grep "NotificationSubscriptionFilter" '; done

Logging into svc-2-mscm
root@svc-2-mscm's password:
ERROR [org.jboss.as.ejb3.invocation] (Thread-281 (HornetQ-client-global-thre →
ads-1396894603)) JBAS014134: EJB Invocation failed on component ModelService →
Helper for method public
com.ericsson.oss.mediation.network.api.util.NotificationSubscriptionFilter c →
om.ericsson.oss.mediation.component.subscription.util.ModelServiceHelper.get →
FilterForNode(java.lang.String):
 javax.ejb.EJBTransactionRolledbackException: No target version information  →
exists for given target model identity 1116-673-999 under the target categor →
y ERBS
Logging into svc-1-mscm
root@svc-1-mscm's password:
[root@ms-1 ~]#
```

3. If the `ossModelIdentity` value is invalid, set it with this command:

```
cmedit set <NodeName> NetworkElement ossModelIdentity=<ossModelIdentity>
FDN : NetworkElement=<NodeName>
1 instance(s) updated
```

4. To force the synchronization of the node, run a manual sync command:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 sync
FDN : NetworkElement=<NodeName>,CmFunction=1
1 instance(s)
```

5. It may take some time for the node to synchronize. Run the following command until the node state changes to SYNCHRONIZED:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED
1 instance(s)
```

5.3 Delay in CPP Node Sync During NE Migration From ENM to ENM

When a large number of CPP nodes are migrated from ENM to ENM there is a delay in CPP sync.

Solution

It is recommended that you migrate the nodes in batches of 1000. Enable CPP sync on all the nodes before enabling the Inventory sync.

Note: Do not run CPP sync and Inventory sync simultaneously.

6 CM Node Synchronization Troubleshooting - CISCO-ASR9000, CISCO-ASR900, JUNIPER-MX, JUNIPER-SRX and JUNIPER-PTX Nodes

> This section provides troubleshooting steps to diagnose common problems with node synchronization and notification handling of CISCO-ASR9000, CISCO-ASR900, JUNIPER-MX, JUNIPER-SRX and JUNIPER-PTX nodes.

6.1 Attempt Manual Sync when CM Node Supervision is Deactivated for CISCO-ASR9000, CISCO-ASR900 and JUNIPER-MX, JUNIPER-SRX and JUNIPER-PTX

Each node that is managed by ENM has an attribute called `CmNodeHeartbeatSupervision.active`. This attribute can be set to `true` or `false` to notify ENM that the node is targeted for supervision or not. Only supervised nodes can be synchronized with ENM.

Prerequisites

— Basic knowledge of how to use the CM CLI.

Steps

1. If the CM supervision of the node is deactivated and a manual synchronization of the node is triggered in the CM CLI the synchronization status of the node will remain `UNSYNCHRONIZED` and no manual syncronizaioton will be executed even if no error message is displayed on CM CLII window.
2. Check if the CM supervision is deactivated for the node, and then activate it.

```
1)     cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    active : false

    1 instance(s)

2)     cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1 act →
ive=true
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1

    1 instance(s)
```

3. Supervision of the node will automatically be triggered in ENM once the value of `CmNodeHeartbeatSupervision.active` changes state from `false` to `true`. It may take some time for the node to synchronize. Execute the below command until the node state changes to `SYNCHRONIZED`.

```
1)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : SYNCHRONIZED

    1 instance(s)
```

Results

The node is synchronized with ENM

6.2 CISCO-ASR9000, CISCO-ASR900, JUNIPER-MX, JUNIPER-SRX and JUNIPER-PTX Nodes Unreachable from ENM

To synchronize with a node, ENM must have a physical connection and the correct network settings between the node and ENM.

The node may be unreachable from ENM for one of the following reasons:

1. ENM specific ports are not available. Refer to page 296.
2. Network connectivity to the node is faulty.
3. The node is stopped, not responding or in an error state. Refer to the *Troubleshooting Guide* in the CPI delivered with the relevant node.
4. The security trust certificates are invalid or incorrect, and permission is denied during CORBA communication handshake between ENM and the node.

Prerequisites

— Root access to the Management Server (MS).

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the CM CLI.

Steps

1. If the node that ENM is attempting to synchronize with is unreachable, sync status will be set to UNSYNCHRONIZED. To check this run the following commands from the CM CLI

```
1)    cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
```

```
    active : true

    1 instance(s)

2)    cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. To confirm that the node is unreachable, the JBOSS logs need to be checked. Log on to the MS and check all MSCM (Mediation Service Configuration Management) JBOSS logs as shown below.

   Note: The error message shown below will only be seen on the MSCM instance that was attempting to synchronize the node.

   The below command when executed will go to all MSCM instances.

   The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in the page 296.

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}' →
); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "Error retrieving moci connection" \
/ericsson/3pp/jboss/standalone/log/server.log* | grep <NodeName>'; done
Logging into svc-2-mscm
2016-02-21 11:08:08,066 ERROR [NO USER DATA, SYNC_NODE.MIB_UPGRADE_DPS_HANDL →
ER_ERROR, ALERT, Flow Engine,\
DPS Database, Error in: MIB UPGRADE DPS HANDLER \
('NetworkElement=LTE03ERBS00033,CmFunction=1'). Reset syncStatus to 'UNSYNCH →
RONIZED'. \
Exception message: Exception has been discovered in the event payload: Error →
 in: READ_TOPOLOGY \
('NetworkElement=LTE03ERBS00033,CmFunction=1'). Error message: Error while r →
etrieving FDNs '. \
Exception message: Error retrieving moci connection: Error occurred while ge →
ttingConfigurationExtended]
Logging into svc-1-mscm
[root@ms-1 ~]#
```

3. If the JBOSS logs above indicate that the problem may be due to a CORBA security communication problem with the node then more detailed logs can be retrieved by following the instructions "*If Issue Suspected on SBI Corba communication for CPP based nodes*" in the page 296.

Results

Possible root causes of synchronization failure identified.

6.3 Troubleshoot CISCO-ASR9000, CISCO-ASR900, JUNIPER-MX, JUNIPER-SRX and JUNIPER-PTX Nodes Synchronization Failure at First Attempt

The first time ENM attempts to synchronize a node, it must calculate the node model identity by reading the Administrative Data (`neProductVersion`) from the node.

If this operation fails, it looks for the `ossModelIdentity` supplied by the operator and uses it to synchronize the node.

If also the `ossModelIdentity` is not present or it is not a valid value, the node cannot be synchronized.

This guide provides information on steps to identify and troubleshoot this issue.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBoss.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Verify that the node synchronization is activated and the sync status is `UNSYNCHRONIZED`. Execute the commands:

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)

2)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. Verify the `nodeModelIdentity` is not set executing the command:

```
cmedit get <NodeName> NetworkElement.nodeModelIdentity
FDN : NetworkElement=<NodeName>
nodeModelIdentity :

1 instance(s)
```

3. One of the reasons the `nodeModelIdentity` is not set is because the node is unreachable.

   To verify and troubleshoot this case, please refer to *Node Unreachable from ENM*

4. If the node is reachable, verify if the security credentials are correctly set. Log on to the ENM MS as the **`litp-admin`** user and switch to the **`root`** user. Check all Mediation Service for Configuration Management (MSCM) JBoss logs using the following commands.

   The command contains sample input, to identify location of vm_private_key, refer to *VM Security Tasks* in the page 296.

```
[root@ms-1 ~]# for i in $(cat /etc/hosts | egrep "mscm\s" | awk '{print $2}' →
); do echo "Logging into ${i}"; \
ssh -i /root/.ssh/vm_private_key cloud-user@${i} \
'grep "Mandatory property username not supplied. Have you set the security c →
redentials when creating the NetworkElement?" \
/ericsson/3pp/jboss/standalone/log/server.log* | grep <NodeName>'; done
Logging into svc-1-mscm
2016-03-09 15:52:26,792 ERROR [com.ericsson.oss.mediation.softwaresync.handl →
ers.CppCalcNodeModelIdHandler] (Thread-76 (HornetQ-client-global-threads-207 →
200151)) NetworkElement=LTE04ERBS00010, SoftwareSyncHandlerException: Error  →
calculating nodeModelIdentity, skip processing (EJBException), EJBException: →
 java.lang.IllegalArgumentException: Mandatory property username not supplie →
d. Have you set the security credentials when creating the NetworkElement?
```

5. If the above ERROR message appears, the security credentials are not correctly set and must be set. To do this, refer to *Create Node Credentials* of the page 296.

6. Force the synchronization of the node by running a manual sync command:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 sync
FDN : NetworkElement=<NodeName>,CmFunction=1

1 instance(s)
```

7. It may take some time for the node to synchronize. Repeat,until the node state changes to SYNCHRONIZED, the command:

```
cmedit get <NodeName> CmFunction.syncStatus
FDN : NetworkElement=<NodeName>,CmFunction=1
syncStatus : SYNCHRONIZED

1 instance(s)
```

Results

User understands the possible root causes of a node failing to synchronize with ENM the first time.

7 Connect to the SGSN-MME Node Troubleshooting

The following task describes the steps to manage Authentication Failure error and to connect to the SGSN-MME node with ENM public-key.

This is not a daily task and must be carried out only when the Authentication Failure condition, reported to the user as an ENM alarm, occurs during the secure connection to the SGSN-MME using the public-key authentication.

Target Groups

— Operator

— Administrator

Task time frame

This task can take about 5-10 minutes.

Prerequisites

— Access to ENM Command Line Interface (ENM CLI) and also to Configuration Management Editor (CMEdit).

— Access to all ENM node logs.

— Access to Alarm Monitoring GUI and has the user rights to manage alarms.

— Node credentials (Secure User Name and Secure User Password) are already created.

— Node is reachable from ENM.

Steps

1. Update Key-Pair operation

   With `secadmin` command the user is able to update ENM public/private ssh keys and copy them to the node.

   Example

   Command syntax:

   ```
   "secadm" ( "sshkey update" | "sku" ) TARGET_NODES [ALGORITHM-TYPE-SIZE]
   TARGET_NODES ::= NODE_LIST | NODE_FILE
   ```

```
NODE_LIST ::= ( "-n" | "--nodelist" ) " " NODE_NAME {"," NODE_NAME}

NODE_NAME ::= <node-name-value> | "NetworkElement="<node-name-value>

NODE_FILE ::= ( "-nf" | "--nodefile" ) " file:"<file-name>

ALGORITHM-TYPE-SIZE ::= ( "-t" | "--algorithm-type-size" ) " " ALGORITHM-NAM →
E-SIZE

ALGORITHM-NAME-SIZE ::= "DSA_1024" | "RSA_1024" | "RSA_2048" | "RSA_4096" | →
"RSA_8192" | "RSA_16384"
```

Example

Command usage:

```
secadm sshkey update -n sgsnselncpcnsgsn57 -t DSA_1024
```

Above command generates DSA key of size 1024.

Example

```
secadm sshkey update -n sgsnselncpcnsgsn57 -t RSA_2048
```

Above command generates RSA key of size 2048.

Result:

```
Sshkey update command executed
```

Note: The user must use the right algorithm type configured on the node. The user can retrieve the configured algorithm type by getting the security node object from ENM.

2. Acknowledge of the error message

   From ENM GUI, the user must acknowledge the error message alarm to clean it from the internal alarm list on the Alarm Monitoring window.

   For more details on how to acknowledge alarms, refer to the *Online Help* of the Alarm Monitoring application.

Results

New public-key is generated and updated on node, then the secure connection with SGSN-MME can be established without failure.

8 Discover a Transport Node Troubleshooting

The goal of this guide is to help troubleshoot issues which may occur during the discovery of following transport network elements:

- Router6672
- Router6675
- Router6x71
- Router6274
- Router6273
- Fronthaul 6080
- MINI-LINK Indoor
- CISCO-ASR9000
- CISCO-ASR900
- JUNIPER-MX
- JUNIPER-SRX
- JUNIPER-PTX
- MINI-LINK-6351
- MINI-LINK-6352
- MINI-LINK-PT2020
- Switch 6391

Prerequisites

Follow the steps in *Connecting to a Virtual Machine* on page 296 and connect to 'mscmip' and 'ipsmserv' Service Group VM.

Troubleshooting

Is the IP address of the node being discovered reachable from ENM server?

Steps

Check if ENM is able to ping the node from mscmip vm.

```
ping <IP address>
```

8.1 Known Errors

Node unreachable by ENM

Issue: The node ENM is attempting to Discover is unreachable. Following could be possible reasons for this:

— Node is in an error state.

Check the state of Node.

— Node unreachable by ENM for CISCO-ASR9000, CISCO-ASR900 , JUNIPER-MX, JUNIPER-SRX, JUNIPER-PTX and FRONTHAUL-6080 (only SNMPv2 case)

  — case SNMPv2: Check if read/write community strings written in Connection Profile and configured on the node are actually matching: if not, autodiscovery will skip the node.

  — case SNMPv3: Check whether User, Authentication mode and key, Privacy mode and key etc. are supported on the node: those profile must be configured and enabled on the node FIRST, then they can be used to fill in the Connection Profile and start auto-discovery. Mind that, in case a single parameter does not match exactly the corresponding string on the node side, auto-discovery task will skip the node.

Make sure the SSH connectivity (port 830 for FRONTHAUL-6080 and port 22 for other nodes) and SNMP connectivity (ports 161 - 162) are enabled.

8.2 Log to check

grep for specific log in mscmip

```
vim /ericsson/3pp/jboss/standalone/log/server.log
```

Sample Error log:

```
Network Element [ < IP address > ] not found
```

Ignore Non-matching NE:

Issue: A node is discovered but not added to the database.

Reason: The NeType of the node discovered does not match the users selection in the Discovery UI.

Log to check: grep for specific log in ipsmserv:

```
vim /ericsson/3pp/jboss/standalone/log/server.log
NeType is not matching for ipaddress : <IP address>
```

Report mis-matching NE

Issue: A node is discovered but not added to the database.

Reason: The discovered node is already in the database with either the same or a different NeType.

Log to check: grep for specific log in ipsmserv:

```
    vim /ericsson/3pp/jboss/standalone/log/server.log
networkElement is already exist's in database with this ipAddress:
```

Skipped NEs:

Issue: A node is discovered but not added to the database.

Reason: The discovered node is already in the database.

Log to check: grep for specific log in ipsmserv:

```
vim /ericsson/3pp/jboss/standalone/log/server.log
IPAddress : <ipAddress> is already in Database with NEType: Router6672.
```

9 TransportCIM Normalization Troubleshooting

9.1 Determine Issues with the TransportCim Normalization Process

Prerequisites

- Nodes supporting normalization.
- Knowledge of TranportCIM normalization process.
- ENM GUI open.
- CLI command knowledge.
- Access to CLI interface.
- Debug process knowledge.

Steps

1. If the TCIM root MO <Network =1> is not present, check the PIB parameter related to the `TransportCIM` normalization:

   If the PIB parameter is disabled, enable the normalization process using the following procedure:

   a. Connect to `ipsmserv` from ms1

   ```
   ssh -i /root/.ssh/vm_private_key cloud-user@svc-3-ipsmserv
   ```

   b. As a root user, run the following command in the `/opt/ericsson/PlatformIntegrationBridge/etc/` folder:

   ```
   config.py update --app_server_address=svc-3-ipsmserv:8080 --name=autoNo →
   rmalizationEnabled --value=true
   ```

2. If the TCIM root MO Network =1 is present, check the `TransportCIM Normalization-state` with the following CLI command:

   ```
   cmedit get Network=1 Node.*
   ```

The Normalization-state can be any of the following:

- `CREATED`: the Normalization process created the node MO under Network=1 and is waiting for the Synchronization of the node to proceed the Normalization of all MOs of the node.
- `RUNNING`: the Normalization process is executing the transformation of MOs .This state is temporary.
- `FAILED`: the Normalization process was not successful.
- `NORMALIZED`: the Normalization process was successful.

3. If the Normalization-state remains CREATED verify the sync status of the node with the following CLI command:

```
cmedit get NetworkElement=<node name> ,CmFunction=1
```

If the node is unsynchronized, force a synchronization on the node, or wait a few minutes to verify if the sync recovers spontaneously.

To force a synchronization on the node run the following CLI command:

```
cmedit action NetworkElement=<node name>,CmFunction=1 sync
```

If the Normalization-state is still CREATED continue to the following steps:

4. If the Normalization-state is FAILED, or does not change to NORMALIZED, perform the following debugging steps to detect the root cause:
    a. connect to ms1
    b. from ms1 connect to ipsmserv
    c. enable log in jboss ipsmserv
    d. run the command:

```
/subsystem=logging/logger=com.ericsson.oss.mediation:add(level=DEBU →
G)
```

    e. open the debug file, and verify the logs.

5. To force normalization on a single node:

```
cmedit action Network=1,Node=<node name> forcedNormalization
```

9.2 Check on TCIM Normalization Feature

> This section provides the troubleshooting steps recommended to check on the TCIM Normalization feature when it is enabled or disabled.

9.2.1 Check on TCIM Normalization Feature when Enabled

Prerequisites

- Knowledge of TranportCIM normalization process
- ENM GUI open
- CLI command knowledge
- Access to CLI interface
- Debug process knowledge

Steps

1. Check the PIB parameter related to the TransportCIM normalization.
    a. Connect to ipsmserv from ms1 (for example: on vAPP, ssh root@192.168.0.42)

    ```
    ssh -i /root/.ssh/vm_private_key cloud-user@<svc_address>-ipsmserv
    ```

    b. As a root user ([cloud-user@svc-3-ipsmserv ~]$ sudo su) give the following command in the:

    ```
    /opt/ericsson/PlatformIntegrationBridge/etc/config.py read --app_se →
    rver_address=<svc_address>-ipsmserv:8080 --name=autoNormalizationEn →
    abled
    ```

2. If `autoNormalizationEnabled` is `true`, all TCIM MOs should be present in DPS database and the TCIM autonormalization is active. To check this via ENM CLI executing the following commands:
    - `cmedit get Network=1`
    - `cmedit get Network=1 Node.*`

    The output must not be 0 instances and the attribute normalization-state of all TCIM Nodes should be NORMALIZED

3. If `autoNormalizationEnabled` value is `true` but the TCIM Network MO is not present (output of the previous CLI commands is `0` instances), then run these steps:

    a. As a root user execute the following command:

    ```
    /opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_address=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=false
    ```

    b. Modify the `autoNormalizationEnabled` value and set it to `true`:

    ```
    /opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_address=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=true
    ```

4. After some time, depending on the number of synchronised networkElement supporting the TCIM normalization, all associated TCIM nodes should be present. To check this via ENM CLI execute the following commands:

    — `cmedit get Network=1`

    — `cmedit get Network=1 Node.*`

    The output must not be `0` instances and the attribute normalization-state of all TCIM Nodes should be NORMALIZED

5. If `autoNormalizationEnabled` value is `false`, no TCIM MOs should be present in DPS and the TCIM autonormalization is not active. To check this via ENM CLI executing the following commands:

    — `cmedit get Network=1`

    — `cmedit get Network=1 Node.*`

    If Network=1 MO is not present: as a root user execute the following command:

    ```
    /opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_address=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=true
    ```

    The normalization process should start automatically.

    If Network=1 MO is present, via ENM CLI execute this command to delete it:

    ```
    cmedit delete Network=1 -ALL –force
    ```

    As a root user execute the following command :

```
/opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_ad →
dress=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=tr →
ue
```

6. After some time, depending on the number of synchronised networkElement supporting the TCIM normalization, all associated TCIM nodes should be present. To check this via ENM CLI execute the following commands:

   — `cmedit get Network=1`

   — `cmedit get Network=1 Node.*`

   The output must not be 0 instances and the attribute normalization-state of all TCIM Nodes should be NORMALIZED

9.2.2 Check on TCIM Normalization Feature when Disabled

Prerequisites

— Knowledge of TranportCIM normalization process

— ENM GUI open

— CLI command knowledge

— Access to CLI interface

— Debug process knowledge

Steps

1. Check the PIB parameter related to the TransportCIM normalization.

   a. Connect to ipsmserv from ms1 (for example: on vAPP, ssh root@192.168.0.42)

   ```
   ssh -i /root/.ssh/vm_private_key cloud-user@<svc_address>-ipsmserv
   ```

   b. As a root user (`[cloud-user@svc-3-ipsmserv ~]$ sudo su`) execute the following command:

   ```
   /opt/ericsson/PlatformIntegrationBridge/etc/config.py read --app_se →
   rver_address=<svc_address>-ipsmserv:8080 --name=autoNormalizationEn →
   abled
   ```

2. If `autoNormalizationEnabled` is `false`, no TCIM MOs should be present in DPS database and the TCIM autonormalization is not active. To check this via ENM CLI, execute the following commands:

- `cmedit get Network=1`
- `cmedit get Network=1 Node.*`

The output must be 0 instances, no Network=1 MO must be present

3. If Network=1 MO is present, via ENM CLI execute this command to delete it:

```
cmedit delete Network=1 -ALL –force
```

4. As a root user execute the following command:

```
/opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_ad →
dress=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=fa →
lse
```

5. If `autoNormalizationEnabled` is `true`, as a root user execute the following command:

```
/opt/ericsson/PlatformIntegrationBridge/etc/config.py update --app_server_ad →
dress=<svc_address>-ipsmserv:8080 --name=autoNormalizationEnabled --value=fa →
lse
```

6. TCIM MOs should be present in DPS database and the TCIM autonormalization is active. To check this via ENM CLI, execute the following commands:

- `cmedit get Network=1`
- `cmedit get Network=1 Node.*`

7. If Network=1 MO is present, via ENM CLI execute the following command to delete it:

```
cmedit delete Network=1 -ALL –force
```

9.3 Deletion of TerminationPoint of NetworkElement

> This section provides the troubleshooting steps recommended to fix common problems when termination point of node is not deleted.

Prerequisites

- Nodes supporting normalization.

— Knowledge of TranportCIM normalization process.

— ENM GUI open.

— CLI command knowledge.

— Access to CLI interface.

— Debug process knowledge.

When the operator is trying to delete the node, although, all links associated with the node are previously deleted, following error is reported.

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 deleteNrmDa →
taFromEnm
 FAILED FDN : NetworkElement=<NodeName>,CmFunction=1
 Error 9999 : Execution Error (Node ID: svc-6-mscm. Exception oc →
curred: There are some Links associated with this Node)
```

In such scenario, check the termination point for the node and execute following steps:

Steps

1. Check the termination points on added node.

   ```
   cmedit get * Node.node-id==<NodeName>, terminationpoint
   ```

2. Delete all the termination point associated for the node.

   ```
   cmedit delete * TerminationPoint.tp-id==*<NodeName>* Terminat →
   ionPoint --force
   ```

3. Execute commands to delete the node.

   Note: To delete the PendingTerminationPoint associated for the node to be deleted, execute the following command:

   ```
   cmedit delete Network=1,Node=<nodeName> PendingTermin →
   ationPoint
   ```

9.4 Link Discovery Troubleshooting for MINI-LINK Indoor Nodes

> This section provides the troubleshooting steps recommended to fix common problems when links are not discovered for MINI-LINK Indoor nodes.

Prerequisites

— MINI-LINK Indoor Nodes supporting normalization.

— Knowledge of TranportCIM normalization process.

— The user is logged on to ENM GUI.

— Basic knowledge of how to use the CM CLI and Network Viewer Application.

— Access to CM CLI Application and Network Viewer Application.

Links configured between MINI-LINK Indoor nodes are not discovered from Network Viewer application.

Steps

1. Logon to ENM GUI and launch Network Viewer application and verify whether links configured between MINI-LINK Indoor nodes are discovered.
2. Identify the network elements for which the links are not discovered.
3. Logon to CM CLI application and execute the following commands to re-sync both the nodes on which the links are not discovered.

```
cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervis →
ion=1 active=false
```

```
cmedit set NetworkElement=<node-name>,CmNodeHeartbeatSupervis →
ion=1 active=true
```

4. Verify that the CM sync status for the network element is in Synchronized state.

```
cmedit get <node-name> CmFunction.syncStatus
```

5. Verify if the links are discovered from the Network Viewer application.

10 Node CLI Launch Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in ENM Node CLI Launch.

Node CLI cannot connect to the node

Possible causes:

1. User has no NodeCLI role.
2. `nodecli` vm is not available.
3. Wrong IP is set for the node.
4. Number of opened sessions reached the maximum.

Steps

1. Steps for case 1:
   - Verify that the user has one of the following user roles: NodeCLI_system_Administrator, NodeCLI_Administrator, NodeCLI_Operator.
   - Login to ENM as Administrator, and add the appropriate user role for this user.
2. Steps for case 3:
   - Update the connectivity info with the right IP address.
3. Steps for case 4:
   - Free a session.

10.1 Node CLI Launch using TACACS/ RADIUS

Possible Causes

1. Incorrect TACACS/RADIUS configuration.
2. Mismatch between ENM and TACACS+ / RADIUS users.
3. SSO not enabled in ENM.

4. Create mandatory node credentials in TACACS/RADIUS.

Scenario: Nodecli launch failed due to incorrect configuration on TACACS+ / RADIUS

1. To allow SSO from ENM, make sure that the TACACS+/RADIUS server is connected and enabled on the node.
2. The configuration of TACACS+/RADIUS is external to ENM. The TACACS+/RADIUS server must be configured correctly by the security administrator.

Scenario: Nodecli launch failed due to mismatch between ENM and TACACS+ / RADIUS users

1. ENM user credentials must be available on the TACACS+/RADIUS server.

   Example

   For a user with name `centralized_user1`, the user name and password must be the same on both the TACACS+/RADIUS server and ENM.

Scenario: Nodecli launch failed as SSO is disabled in ENM

1. Check the SSO authentication status in ENM using the `secadm` SSO command.
2. Remote authentication of TACACS/ RADIUS server does not work if SSO is disabled, therefore you must enable SSO.

Scenario: Nodecli launch failed due to node credentials not present on TACACS/ RADIUS server

1. Check whether the mandatory node credentials are present on the TACACS +/RADIUS server. Node credentials that are mandatory in ENM while adding a node can be secure user, normal user, root user or nodecli user. These mandatory users are different for each node type.

   For example, if a secure user is mandatory, then secure user credentials must be present in the TACACS+/RADIUS server.

11 CM Events Troubleshooting

This section provides the troubleshooting steps recommended to diagnose, and fix common problems with CM Events NBI.

11.1 Processing Events

CM events from mediation are processed by a service group called `dchistory`. As this service group operates across multiple instances, It may be necessary to log in to both service group instances to verify that events are being processed correctly.

Prerequisites

Physical deployment Prerequisites:

— Access to Management Server (MS)

— Access to the Service Cluster nodes

— Access to the ENM Command Line Interface (CLI)

Cloud deployment Prerequisites:

— Access to the private key file for authentication. Contact your Openstack administrator

— Access to the Ericsson Management Portal (EMP) VM in the ENM on Cloud deployment

— Access to the ENM Command Line Interface (CLI)

Steps

1. To log on to `dchistory` as root user, refer to *Connecting to a Virtual Machine* in page 296.
2. Check the JBoss logs for any errors or exceptions in `dchistory`, refer to *Collect JBOSS Logs* in page 296.
3. If notifications are being processed, then a file is generated in the directory `/ericsson/enm/cm_events_nbi/data`.

   Note: A file only exists in this directory while notifications are being loaded into its data store location. This can be defined in the order of seconds. When notifications are successfully loaded, the file no longer exists.

4. If notifications are not being processed, then the following checks should be carried out:

   Note: The `lcmserv` service group is online is a prerequisite to this step.

   Log on to each `lcmserv` VM as root user, refer to *Connecting to a Virtual Machine* in page 296.

5. Check that JBoss is running, using the command below:

```
[root@svc-2-lcmserv ~]# service jboss status
jboss-as is running
```

6. Check the JBoss logs for the following messages.

   Messages appear periodically separated by five minute intervals, as shown below:

```
2016-03-19 23:10:24,704 INFO  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 91) LicenseManagerBean.validatePermission() called  →
for license: FAT1023443, permission returned: ALLOWED
2016-03-19 23:15:24,050 INFO  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 19) LicenseManagerBean.validatePermission() called  →
for license: FAT1023443, permission returned: ALLOWED
2016-03-19 23:20:24,060 INFO  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 70) LicenseManagerBean.validatePermission() called  →
for license: FAT1023443, permission returned: ALLOWED
```

   If the above message reporting is seen then the license required for event processing has been provided. However, if messages like the following are seen, it indicates licensing has not been provided and event processing does not occur.

```
2016-03-19 23:25:24,046 WARN  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 115) LicenseManagerBean.validatePermission() called →
 for license: FAT1023443, permission returned: DENIED_NO_VALID_LICENSE
2016-03-19 23:30:24,046 WARN  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 115) LicenseManagerBean.validatePermission() called →
 for license: FAT1023443, permission returned: DENIED_NO_VALID_LICENSE
2016-03-19 23:35:24,046 WARN  [com.ericsson.oss.services.lcm.impl.LicenseMan →
agerBean] (EJB default - 115) LicenseManagerBean.validatePermission() called →
 for license: FAT1023443, permission returned: DENIED_NO_VALID_LICENSE
```

7. On `dchistory`, check that the file permissions are correct for the json files in `/ericsson/enm/cm_events_nbi/data`

   They should be as follows for the jboss_user(644):

```
[root@svc-2-dchistory]# ls -lart /ericsson/enm/cm_events_nbi/data
drwxr-xr-x. 3 root       root   4096 May  4 18:12 ..
-rw-r--r--. 1 jboss_user jboss 20296 May  5 16:19 c9cd918e-0689-4a5a-840f-05 →
fd70ab8fa2_2016-05-05T16:19:17.701Z.json
drwx------. 2 jboss_user jboss  4096 May  5 16:19 .
```

   Refer to the page 296 for details on adding a license.

Note: The license status is checked every five minutes. If the license is modified, the new license status does not apply until the subsequent license status check.

Results

CM events are processed correctly.

Note: DPS can go into Read Only mode for a number of reasons. If DPS is in Read Only mode, CM Events can no longer be relied upon to forward CM notifications north bound to requesting applications. However, when the database is returned back to Read/Write mode, nodes will automatically be re-synchronized with ENM and CM Events will receive all the notifications from the node synchronization and therefore will be up to date with all changes since DPS went into Read Only mode. There should be no need for user or system administrator intervention.

11.2 Loading Events to Data Store

CM events from mediation are processed by a service group called `dchistory`. This service group operates across two blades in a master-slave configuration, with the master service group processing events. The events are loaded into the data store maintained in the service group `solr`. The data is stored in a specific `Solr core` referred to as `cm_events_nbi`.

The temporary location `/ericsson/enm/cm_events_nbi/data` is usually empty or contains few files, but there can be a scenario when a large volume of files is being produced and not periodically deleted and this could indicate a failure to successfully store them.

Prerequisites

Physical deployment prerequisites:

— Access to Management Server (MS)

— Access to the Service Cluster nodes

— Access to the ENM Command Line Interface (CLI)

Cloud deployment prerequisites:

— Access to the private key file for authentication. Contact your OpenStack administrator

— Access to the Ericsson Management Portal (EMP) VM in the ENM on Cloud deployment

— Access to the ENM Command Line Interface (CLI)

All steps described in Processing Events on page 72 are performed.

Steps

1. Check the temporary location `/ericsson/enm/cm_events_nbi/data` and if there are files older than one minute go to *step 2*.
2. Log on to each `solr` VM as `root` user, refer to section *Connecting to a Virtual Machine* in ENM Troubleshooting Guide.
3. Collect the `solr` logs and check for errors.

```
/ericsson/enm/solr/cm_events_nbi/data/tlog/tlog* on each solr VM
/ericsson/solr/install/solr-4.8.1/enm/logs/solr* on each solr VM
/var/log/messages on each solr VM
```

   If no errors are seen, CM events are loaded successfully into the data store.

4. If any of the following log message is present in the logs, restart the solr VM.

```
org.apache.solr.common.SolrException; java.lang.ArrayIndexOutOfBoundsExcepti →
on
Caused by: java.io.IOException: Stale file handle
```

   Do the following steps to restart the solr VM:

   a. Stop solr by running the following command.

```
[root@svc-3-solr cloud-user]# service solr stop
SOLR: INFORMATION (): Solr script called with the argument:stop
    SOLR: INFORMATION (): stopping solr process called with the user root
    SOLR: INFORMATION (): Stopped solr process with pid : 4974
```

   b. Check status of solr by running the following command.

```
[root@svc-3-solr cloud-user]# service solr status
SOLR: INFORMATION (): Solr script called with the argument:status
   SOLR: INFORMATION (): solr pid file does not exists,setting solr pid file
   dead but pid file exists
   SOLR: INFORMATION (): Current status of solr is: 1
```

   c. Start solr by running the following command.

```
[root@svc-3-solr cloud-user]# service solr start
SOLR: INFORMATION (): Solr script called with the argument:start
SOLR: INFORMATION (): About to start the solr DB service
SOLR: INFORMATION (): SOLR data SFS mount available: /ericsson/enm/solr
SOLR: INFORMATION (): SOLR Data directory exists at : /ericsson/enm/solr/data →

SOLR: INFORMATION (): Successfully set data directory permissions on /ericsso →
n/enm/solr/data
SOLR: INFORMATION (): Deleted tlogs for /ericsson/enm/solr/cm_events_nbi/data →
/tlog/
SOLR: INFORMATION (): Deleted tlogs for /ericsson/enm/solr/data/tlog/
SOLR: INFORMATION (): Heap memory to be assigned for Solr is: 1024
SOLR: INFORMATION (): Started solr process with pid : 12846 12846
```

5. If there are other exceptions, check the health of the `Solr cm_events_nbi` core. Go to following directory:

```
[root@svc-1-solr index]# cd /ericsson/solr/install
```

Run the following command.

```
[root@solr install]# ./SolrIndexUtility.sh checkIndex /ericss →
on/enm/solr/cm_events_nbi/data/index
```

If the core is healthy, the following message is displayed at the bottom of the output:

```
No problems were detected with this index.
```

If the following warnings are displayed:

Note: The numbers in the output may be different.

```
WARNING: 1 broken segments (containing 2 documents) detected

WARNING: would write new segments file, and 2 documents would →
 be lost, if -fix were specified
```

Search for the `CorruptedIndexException` exception if it is present run the following command to remove the whole `cm_events_nbi` core:

```
[root@solr install]# ./purgeSolrData.sh cm_events_nbi
```

6. If there are no exceptions, `cm_events_nbi` can be still cleaned manually.

   There are two ways for purging CM events from the database using the `purgeSolrData.sh` script: delete all records and delete records on time basis.

Option	Description
Delete All Records	`/ericsson/solr/install/ purgeSolrData.sh cm_events_nbi`
Delete Records on Time Basis	`/ericsson/solr/install/ purgeSolrData.sh cm_events_nbi <Number of younger days to retain>` Example of command to retain the data of the six days young and remove the history data older than six days.

Option	Description
	`/ericsson/solr/install/purgeSolrData.sh cm_events_nbi 6`

Results

Writing CM events is achieved.

11.3 Reading Events

CM Events NBI is executed by a service group called `cmevents`. This service group operates across two blades in an active-active configuration, with processing of event requests evenly distributed.

Prerequisites

Physical deployment Prerequisites:

— Access to Management Server (MS)

— Access to the Service Cluster nodes

— Access to the ENM Command Line Interface (CLI)

Cloud deployment Prerequisites:

— Access to the private key file for authentication. Contact your Openstack administrator

— Access to the Ericsson Management Portal (EMP) VM in the ENM on Cloud deployment

— Access to the ENM Command Line Interface (CLI)

Steps

1. Connect to each `cmevents` VM instance, refer to *Connecting to a Virtual Machine* in page 296.
2. Check that JBoss is running, using the command below:

```
[root@svc-1-cmevents ~]# service jboss status
jboss-as is running
```

3. Check the JBoss logs for any errors or exceptions, refer to *Collect JBOSS Logs* in page 296.

Results

CM Events NBI requests are being processed correctly.

12 Bulk Export Troubleshooting

This section contains the recommended troubleshooting procedures to perform to diagnose and fix issues which may occur with the Bulk Export feature on the ENM system.

— To monitor and free up disk space for exports, follow the instructions in the section *Reduce System Usage for Shared File System for Bulk Export* in page 296.

  A typical scenario would be when the shared file system exceeds 90% capacity, and new exports are failing with the message "`Error 8028: Insufficient disk space available for export job on {0}`".

— For troubleshooting related to the `impexpserv` Virtual Machine (VM), follow the instructions in the sections *Basic Troubleshooting with the VM(s)*, and *Check the Status of All Deployed Virtual Machines*, in page 296.

— To unblock unwanted exports which are stuck in a 'STARTED' or 'STARTING' state, refer to Bulk Export - Unblock Jobs Troubleshooting on page 79.

  A typical scenario would be when the threshold for parallel exports has been reached, and new exports are failing with the message "`Error 8027: The server is currently busy due to a high number of exports`".

12.1 Bulk Export - Unblock Jobs Troubleshooting

— These steps will set ALL bulk exports which are in a 'STARTED' or 'STARTING' state to a 'FAILED' state.

— Steps must be performed on any one of the active `impexpserv` instances (eg. svc-1-impexpserv).

— Perform these steps when `unwanted exports` are stuck in a 'STARTED' or 'STARTING' state.

— A typical scenario would be when the threshold for parallel exports has been reached and new exports are failing with the message "`Error 8027 : The server is currently busy due to a high number of exports`".

Prerequisites

Physical deployment Prerequisites:

— Access to Management Server (MS)

— Access to the Service Cluster nodes

— Access to the ENM Command Line Interface (CLI)

Cloud deployment Prerequisites:

— Access to the private key file for authentication. Contact your Openstack administrator

— Access to the Ericsson Management Portal (EMP) VM in the ENM on Cloud deployment

— Access to the ENM Command Line Interface (CLI)

Steps

1. Determine the hostnames of the `impexpserv` instances.

    a. On a physical deployment, run the following command from the MS:

    ```
    [root@ieatlms4400 ~]# cat /etc/hosts | grep impexpserv
    10.247.246.53    svc-2-impexpserv    impexpserv-2-internal    # Cre →
    ated by LITP. Please do not edit
    10.247.246.52    svc-1-impexpserv    impexpserv-1-internal    # Cre →
    ated by LITP. Please do not edit
    ```

    b. On a cloud deployment, run the following command from the EMP VM:

    ```
    [root@gat-emp-0 ~]# consul members list | grep impexpserv
    gat-impexpserv-0         10.5.1.91:8301   alive   client  0.8.1  2   →
            dc1
    gat-impexpserv-1         10.5.1.92:8301   alive   client  0.8.1  2   →
            dc1
    ```

2. To log on to one of these VMs as root user, refer to *Connecting to a Virtual Machine* in *ENM System Troubleshooting Guide*.

3. Disable the update blocked jobs mechanism (this is done to allow new parameters to be set).

    ```
    [root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
    g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
    =scheduledUpdateBlockedJobsEnabled --value=false service_identifier=export-s →
    ervice --app_server_identifier=svc-2-impexpserv
    ```

4. Temporarily change the settings for the unblocking mechanism to run 1 minute after enabling (see step 5).

    ```
    [root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
    g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
    =scheduledUpdateBlockedJobsHour --value='*' service_identifier=export-servic →
    e --app_server_identifier=svc-2-impexpserv

    [root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
    g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
    =scheduledUpdateBlockedJobsMinute --value='*' service_identifier=export-serv →
    ice --app_server_identifier=svc-2-impexpserv

    [root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
    ```

```
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsTime --value='1' service_identifier=export-servic →
e --app_server_identifier=svc-2-impexpserv

[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsUnit --value='MINUTES' service_identifier=export- →
service --app_server_identifier=svc-2-impexpserv
```

5. Enable the unblock jobs mechanism.

```
[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsEnabled --value=true service_identifier=export-se →
rvice --app_server_identifier=svc-2-impexpserv
```

6. Wait for one minute and confirm that the jobs have been set to a 'FAILED' state using the ENM CLI command '`cmedit export -st`'.

7. Disable the update blocked jobs mechanism (to allow default settings to be restored).

```
[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsEnabled --value=false service_identifier=export-s →
ervice --app_server_identifier=svc-2-impexpserv
```

8. Restore defaults.

```
[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsHour --value='*/2' service_identifier=export-serv →
ice --app_server_identifier=svc-2-impexpserv

[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsMinute --value='0' service_identifier=export-serv →
ice --app_server_identifier=svc-2-impexpserv

[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsTime --value='5' service_identifier=export-servic →
e --app_server_identifier=svc-2-impexpserv

[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsUnit --value='HOURS' service_identifier=export-se →
rvice --app_server_identifier=svc-2-impexpserv
```

9. Enable the unblock jobs mechanism.

```
[root@svc-2-impexpserv ~]$ /opt/ericsson/PlatformIntegrationBridge/etc/confi →
g.py update --app_server_address=svc-2-impexpserv:8080 --scope=GLOBAL --name →
=scheduledUpdateBlockedJobsEnabled --value=true service_identifier=export-se →
rvice --app_server_identifier=svc-2-impexpserv
```

Results

No exports will remain in a 'STARTED' or 'STARTING' state. Further exports can be started successfully.

12.2 Bulk Export - MINI-LINK Indoor Nodes Missing Troubleshooting

— These steps will identify the Network Element(s) which are missed during export and resolve the issue for those Network Element(s).

— Steps must be performed on the active `impexpserv` instances (for example, svc-1-impexpserv).

— A typical scenario would be when the Export Job status reports some nodes as missing. For example:. `"COMPLETED Completed with {1} node(s) missing"`

Prerequisites

Physical deployment Prerequisites::

— Access to Management Server (MS)

— Access to the Service Cluster nodes

— Access to the ENM Command Line Interface (CLI)

Cloud deployment Prerequisites:

— Access to the private key file for authentication. Contact your Openstack administrator

— Access to the Ericsson Management Portal (EMP) VM in the ENM on Cloud deployment

— Access to the ENM Command Line Interface (CLI)

Steps

1. Determine the host names of the`impexpserv` instances.

    a. On a physical deployment, run the following command from the MS:
    ```
    [root@ieatlms4400 ~]# cat /etc/hosts | grep
    impexpserv10.247.246.53 svc-2-impexpserv impexpserv-2-
    internal # Created by LITP. Please do not
    edit10.247.246.52 svc-1-impexpserv impexpserv-1-
    internal # Created by LITP. Please do not edit
    ```

    b. On a cloud deployment, run the following command from the EMP VM:
    ```
    [root@gat-emp-0 ~]# consul members list | grep
    impexpservgat-impexpserv-0 10.5.1.91:8301 alive client
    0.8.1 2 dc1gat-impexpserv-1 10.5.1.92:8301 alive client
    0.8.1 2 dc1
    ```

2. To log on to one of these VMs as root user, refer to Connecting to a Virtual Machine in ENM System Troubleshooting Guide.
3. Copy the impexpserv server.log using the below steps on each impexpserv VM to Management Server.
    a. `cd /ericsson/3pp/jboss/standalone/log`
    b. `scp server.log root@ms-1:/var/tmp`
4. Search the log file for the error message 'com.ctc.wstx.exc.WstxIOException: Invalid null character in text to output'.
    a. Example: `2020-01-14 01:00:07,919 ERROR [com.ericsson.oss.services.cm.export.transformer.service.ejb.ThreeGppTransformer] (Batch Thread - 10) Transformer ExceptionInvalid null character in text to output: [ManagedElement=CN-23139-27400-1] for export job Id: [401] caused by: [java.io.IOException: Invalid null character in text to output] : com.ctc.wstx.exc.WstxIOException: Invalid null character in text to output`
    b. Make a note of the ManagedElement Name from the log message. In above example it will be 'CN-23139-27400-1'
5. Perform Manual sync for the ManagedElement which reported the error in step 4.
    a. Login to ENM Command Line Interface (CLI)
    b. Execute the below command of manual sync`cmedit action NetworkElement=<NetworkElementName> CmFunction=1 sync`Example:`cmedit action NetworkElement=CN-23139-27400-1 CmFunction=1 sync`
    c. Network Element Sync Status to be in SYNCHRONIZED state. Check the status in ENM CLI using below command:`cmedit get NetworkElement=<NetworkElementName>,CmFunction=1`Example:`cmedit get NetworkElement=CN-23139-27400-1 CmFunction=1`
6. Run the Export job for this Network Element and it must be successful.

Results

Export job must be successful without any node in missing state.

12.3 502 Gateway Timeout Errors When Creating Bulk Export Jobs

— If an operator attempts Bulk Export job request using REST interface, it is possible that the job creation is active in the backend but not promptly

reported back to the operator. This leads to a 502 gateway timeout error. In this case, operator can check the job status to assert the successful job creation. If not, the export request must be retried.

— If a Bulk Export job request is attempted from the CLI, it is possible that the job creation is active in the backend but response is not received for a long time (CM CLI looks like in a loading state and hung to the user or the operator). In this case, operator can check export status command to confirm the job creation. If not, the export request must be retried.

13 AMOS Troubleshooting

> This section provides the troubleshooting steps recommended to diagnose, and fix, common problems in the ENM Advanced MO Scripting (AMOS), or in the Shell Terminal service.

13.1 AMOS or Shell Terminal Link Unavailable from ENM Launcher

The `Advanced MO Scripting` or the `Shell Terminal` link is not available when logged into the ENM UI.

Steps

1. Verify that the user has either `Amos_Administrator` or `Amos_Operator` user roles
2. Log on to ENM as Administrator, and add the appropriate user role to the user.

13.2 AMOS or Shell Terminal Fails to Launch with Authentication Failed Dialog

The Authentication Failed dialog is displayed when a user with AMOS roles tries to start the Advanced MO Scripting (AMOS) or the Shell Terminal (SSH) from the ENM Launcher. To check this issue, verify that `nslcd` service is running on all AMOS VM's.

Steps

1. Follow the instructions in *Connect to a Virtual Machine* in page 296, then log on to the `amos` VM.
2. Check the status of service `nslcd`:

   ```
   service nslcd status
   ```

   If the service `nslcd` is running the user will see:

   ```
   nslcd (pid  5030) is running...
   ```

   If it is not:

```
nslcd is stopped
```

3. If service `nslcd` is not running on any of AMOS VM's, start the service:

   ```
   service nslcd start
   ```

   The system will show similar output to:

   ```
   nslcd (pid  5030) is running...
   ```

13.3 AMOS Fails to Launch with License Error Dialog

A dialog with the License Error message is displayed when Advanced MO Scripting (AMOS) is started from the ENM Launcher without the AMOS licensed installed in ENM.

Steps

1. Verify that FAT1023078, FAT1023599, or both licenses are installed.
2. Log on to ENM as Administrator, then use the Command Line Interface (CLI) application to install the license.

13.4 Enable AMOS and Shell Terminal in an iPad

The Amos and Shell Terminal uses a Secure WebSocket, and Safari browser requires a certificate from a trusted signing authority for use this Secure WebSocket. Launching Amos and Shell Terminal on an iPad therefore requires a valid certificate for ENM.

The certificate needs to be installed the first time that AMOS or Shell Terminal is launched in the iPad, or in the ENM installation.

Note: Safari is the only browser that allows the export of a valid certificate to an iPad.

Prerequisites

— Amos_Administrator role.

— Amos_Operator role.

— ADMINISTRATOR role.

Steps

1. To learn how to obtain a valid certificate for ENM, refer to *"Export ENM PKI Root CA Certificate*" section, in page 296.

   Note: When running the Exporting Certificate steps on an iPad, the system will automatically request installation of the certificate.

13.5 Firefox Copy and Paste Limitations

When you launch ENM Advanced MO Scripting (AMOS) using Firefox web browser, it is not possible to paste with the mouse on Firefox.

Prerequisites

— Amos_Administrator role.

— Amos_Operator role.

Steps

Copy and paste with keyboard shortcuts **`Ctrl+Insert`** / **`Shift+Insert`**.

Results

The user knows about Firefox copy and paste limitations.

13.6 AMOS or Shell Terminal session times out with 'Connection Lost' Dialog

The 'Connection Lost' Dialog is displayed when SSH session is idle timed out after a defined time.

1. Follow the instructions given in the *Configure Timeout on SSH Sessions* section of the 'ENM Configuration System Administrator Guide to check the defined timeout for web socket sessions.

13.7 Total No. of MOs on ENM CLI Differs from Total No. of MOs on AMOS

The total number of MOs returned using the `lt all` command from the ENM CLI differs from that returned when using the same command from AMOS.

This happens because the user has connected to the node in different ways. Both of the following security connection types were used:

— Transport Layer Security (TLS)

  The ENM CLI offers this connection type as an option when launched. AMOS can be forced to use this connection type if the following arguments are specified:

  - `-v comcli=27`
  - `-v comcli=28`

— Secure Shell (SSH)

  The ENM CLI offers this connection type as an option when launched. AMOS chooses this connection type by default.

  If the user connects to the node using TLS with one tool, and using SSH with the other, the number of MOs returned can differ.

Prerequisites

— `Element_Manager` role

— `Amos_Administrator` role

— `Amos_Operator` role

Steps

To ensure consistency, use the same connection type (either SSH or TLS) when running the `lt all` command.

13.8 AMOS Command is Showing Different Output from Different VMs for Same Node

Sometimes the number of MOs displayed in the output is not same when command is executed from different VMs for same node. This happens when AMOS fails to communicate with node to download the correct MOM file, resulting in a corrupted MOM file being created.

For example:

Number of MOs from output of command "st mme" or "st cell" is zero on one of the amos/scripting VM.

Output of command "pst" is different on one of the amos VMs.

Steps

1. Follow the instructions in Connect to a Virtual Machine, then log on to the affected AMOS/Scripting VM.

2. Delete the MOM file referred by AMOS session.

    a. Get the name of MOM file from AMOS output;

    For example:

    Checking MOM
    version...MSRBS_NODE_MODEL_18.Q1_337.656.39_6c80_GW

    b. Delete MOM files using following command:

    ```
    rm -f /opt/ericsson/amos/moshell/jarxml/<MOM_file_name>*.gz
    ```

    Example:

    ```
    rm -f /opt/ericsson/amos/moshell/jarxml/MSRBS_NODE_MODEL_18.Q1_337.
    656.39_6c80_GW*.gz
    ```

13.9 AMOS Command is Showing Error: 'User does not have permission to run COLI commands' in the Output

Error 'User does not have permission to run COLI commands' is displayed when any COLI command is executed after connecting AMOS to a COM node and required roles are missing.

1. Follow the instructions in document 'Manage Security' 18/1553-LZA 701 6014, Section - 'Roles only for Ericsson Troubleshooting', to see which roles are required and create the roles if not already created.

13.10 AMOS Command is Showing SSLHandshakeException Error in the Output

Some nodes may support TLSv1 and other may support TLSv1.2. Having mismatched TLS protocols on the client/server can lead to SSL Handshake Exception. In this case you may need to set the TLS version to TLSv1.2.

Steps

1. Follow the instructions in 'ENM Security System Administrator Guide' 2/1543-AOM 901 151-2, Section 'TLS Protocol Version Update'.

13.11 AMOS and Element Manager Limitations

AMOS and Element Manager have the following limitations:

— Multimode feature in AMOS is only supported in the CPP based nodes.

— AMOS or Element Manager cannot be launched from Network Explorer or Topology Browser if MO below Managed Element is selected for any node type as the `netype` is not available for that MO.

— Shell terminal, AMOS, or any application launched from the Cendio desktop cannot function on any iOS Device updated to the iOS version 10.3.1 or 10.3.2.

14 EM-GUI Troubleshooting Guide

> This section provides the troubleshooting steps recommended to diagnose and fix common problems when launching Element Manager-GUI (EM-GUI).

14.1 EM-GUI launch displays 'Secure Connection Failed' error message

EM-GUI launch fails when Firefox browser is opened on Cendio Desktop, and it displays the following message:

```
Secure Connection Failed
An error occurred during a connection to <NODE IP>:8443. SSL peer was unable to negotiate an acceptable set of security parameters.
(Error code: ssl_error_handshake_failure_alert)
The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
Please contact the website owners to inform them of this problem.
```

Prerequisites

— User has one of the following Roles:

- Network_Explorer_Operator.
- Network_Explorer_Administrator and Element_Manager_Operator.
- Element Manager Capabilities.

— PKI Entity is created.

— Ensure the user certificates and the node certificates match, so they have the same CA and they share the same chain of certificates.

Steps

1. Log on to ENM as Administrator.
2. Check if the user has the required roles.

   Note: Refer to *User Management* application in the *ENM online help* to check this.

   If not, add the appropriate role to this user.

3. If PKI Entity is not present, refer to sections *Configuring Users to Access AMOS and Element Manager, and WinFIOL towards SL2* or *TLS Enabled Nodes* in page 296 to learn how to create it.
4. Verify that user is trying to launch EM-GUI from `Network Explorer` for a node with the neType equal to 'RadioNode'
5. Verify that user searched the node in Network Explorer using one of the these keywords: `NetworkElement`, `MeContext`, `ManagedElement`

Results

EM-GUI is launched successfully.

14.2 EM-GUI Launch Fails After Cendio Desktop is Opened

EM-GUI launch can fail after Cendio Desktop is opened due to '`TLS misconfiguration`' or '`port 8443 is not available`' issues. In this scenario, the system shows one of these messages: '`Failed to fetch the certificate for user <user>`' or '`Error while evaluating certificates`'. Follow the below steps to troubleshoot this issue.

Prerequisites

— Network_Explorer and Element_Manager_Operator role or Element Manager Capabilities.

— PKI Entity is created.

— Understanding of TLS standard, and how it is used for mutual authentication.

— Understanding of how the MOs setup works.

Steps

1. Log on to ENM as Administrator.
2. Check if the user has the required roles.

   Note: Refer to *User Management* application in the *ENM Online Help* to check this.

   If not, add the appropriate role to the user.
3. Check if user's PKI Entity exists.

   Refer to *PKI Entity Management* application in the *ENM online help* to check this.

a. If PKI Entity is not present, refer to *Configuring Users to Access AMOS and Element Manager, and WinFIOL towards SL2* or *TLS Enabled Nodes* in page 296 to learn how to create it.

b. If PKI Entity certificate or OTP Token expired

   i. Remove PKI Entity

   ii. Recreate PKI Entity according to *Configuring Users to Access AMOS and Element Manager, and WInFIOL towards SL2* or *TLS Enabled Nodes* in page 296.

4. Verify that CA certificate that was used to generate user's certificate is still valid, and is present on the node.

   For more information on CA certificates, refer to Section *Public Key Infrastructure System* in page 296.

5. Verify that the below MOs are properly set:

```
ManagedElement=<NODENAME>,SystemFunctions=1,SysM=1,HttpM=1,Https=1
ManagedElement=<NODENAME>,SystemFunctions=1,SysM=1,NetconfTls=1
ManagedElement=<NODENAME>,SystemFunctions=1,SysM=1,CliTls=1
```

   For more information on MO Configuration, refer to section *Manage Security* in page 296.

Results

EM-GUI is launched after the Remote Desktop Viewer is opened.

14.3 Error Launching Element Manager without Certificate Installed

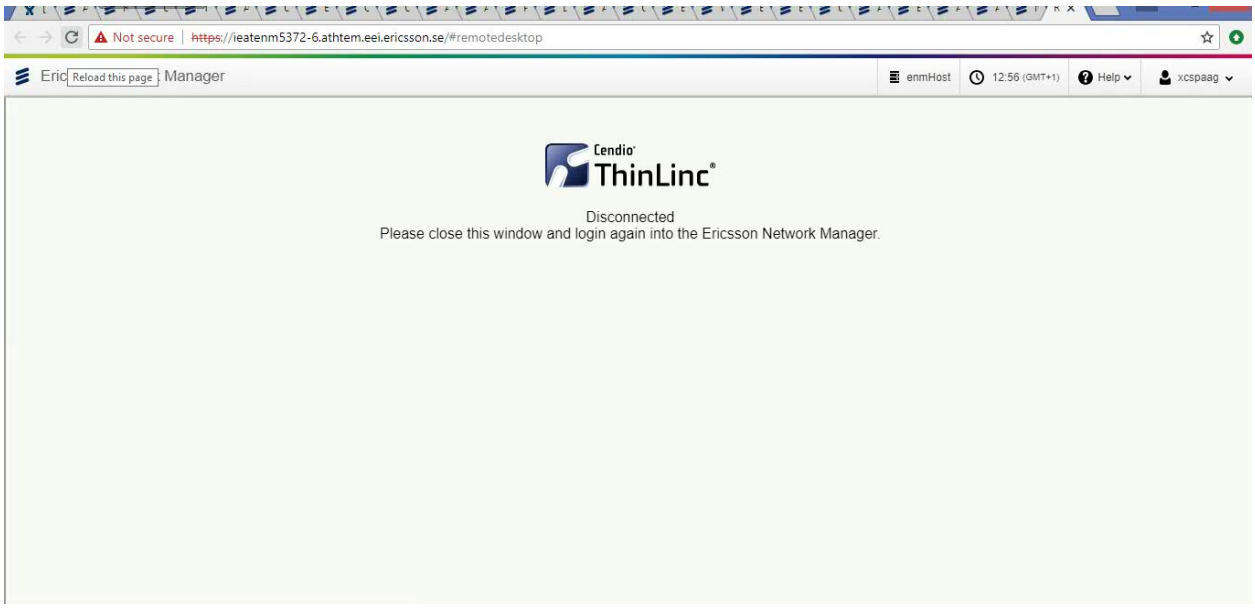


Figure 2 Element Manager Launch Error

When launching Element Manager without certificate installation, launch fails with an error message as per Figure 2.

This is due to certificates not being installed prior to attempting to launch Element Manager.

Workaround

User may need to contact an administrator to close unused Cendio Desktops session.

Remedy

Install an SIS Server Certificate to Enable Launch of Element Manager from Network Explorer Over HTTPS

This procedure shows the operator how to install a Site Infrastructure (SIS) server certificate for MSC-S BC (with APG43 Linux) (IS) (MSC-BC-IS) on the management host.

The certificate ensures the operator can launch the Element Manager using the HTTPS protocol after selecting a node for the first time in Network Explorer. On completing the procedure, the operator can expect to view the Integrated Site Management System welcome page in the Cendio Thinlinc desktop.

Prerequisites

This user is assigned either the Network_Explorer and Element_Manager_Operator roles, or the Element Manager Capabilities role.

Steps

1. Select a node in Network Explorer.
2. From the Actions menu, in the far right hand side of the menu bar, select **Launch Element Manager**.

   The Choose Encryption page is launched in Cendio Thinlinc desktop. The onscreen text indicates that, for first-time use of the HTTPS protocol when launching Element Manager for a particular node, a certificate must be installed.
3. Choose the action that matches your scenario.

Option	Description
I want to use HTTP	Click **Continue over HTTP**.
I want to use HTTPS. This is the first time I have launched Element Manager over HTTPS for the selected node, so I need to install a certificate.	Click **Install Certificate**. Select all check boxes in the Downloading Certificate popup, and click **OK**. The system installs the SIS server certificate on the management host.
I want to use HTTPS. I have successfully launched Element Manager for the selected node over HTTPS before.	Click **Continue over HTTPS**.

4. Ensure that the MSC-S BC (with APG43 Linux) (IS) welcome page is displayed.

   If it is not, contact Ericsson support.
5. Click **Log In** to provide node credentials.

14.4 Launch Element Manager Button not Available for RadioNode

The **Launch Element Manager** button is not available when user searches and selects a node with the `neType` equal to `RadioNode` from Network Explorer.

Prerequisites

— One of the following Roles:

- Network_Explorer_Operator.
- Network_Explorer_Administrator and Element_Manager_Operator.

- Element Manager Capabilities.

Steps

1. Log on to ENM as Administrator.
2. Check if the user has the required roles.

   Note: Refer to *User Management* application in the *ENM online help* to check this.

   If not, add the appropriate role to this user.
3. Verify that user is trying to launch EM-GUI from Network Explorer application for a node with the `neType` equal to `RadioNode`.
4. Verify that user searched the node in Network Explorer using one of the these keywords: `NetworkElement`, `MeContext`, `ManagedElement`.

Results

The **Launch Element Manager** button is available from Network Explorer when a node with the neType equal to 'RadioNode' is selected.

14.5 Shell Terminal on Scripting Link is Missing from ENM Launcher

> In the ENM Launcher, no **Shell Terminal on Scripting** link is displayed to the user.

Prerequisites

The user performing the troubleshooting has been assigned the `Administrator` role.

Steps

1. In the **User Management** application, verify that the user has either of the following roles:
   - `Scripting_Operator`
   - A custom role with the following permissions:
     - `scripting_cli_access`
     - `scripting_cron_service`

2. Log on to ENM as Administrator and, in the **Role Management** application, add the appropriate user role to the user.

14.6 Shell Terminal on Scripting Link Fails to Launch with Authentication Failed Dialog

When a user clicks the **Shell Terminal on Scripting** link on the **ENM Launcher**, the **Authentication Failed** dialog is displayed. To resolve this issue, ensure that the `nslcd` service is running on all scripting virtual machines.

Steps

1. Follow the instructions in the Connect to a Virtual Machine on page 2 section, then log on to the scripting VM.
2. Check the status of the `nslcd` service:

   ```
   service nslcd status
   ```

   If the `nslcd` service is running, the following message displays:

   ```
   nslcd (pid 5030) is running...
   ```

   If the `nslcd` service is not running, the following message displays:

   ```
   nslcd is stopped
   ```

3. If the `nslcd` service is not running on any of scripting virtual machines, start the service:

   ```
   service nslcd start
   ```

   A message similar to the following message displays:

   ```
   nslcd (pid 5030) is running...
   ```

15 Element Manager and Cabinet Viewer Troubleshooting

This section provides the troubleshooting steps recommended to diagnose, and fix common problems in ENM Element Manager.

15.1 Element Manager or Cabinet Viewer Desktop not Opening

Cendio desktop does not open.

Prerequisites

— Assigned the roles: Element_Manager_Operator, Network_Explorer_Operator.

Steps

1. Follow the instructions in the *Connect to a Virtual Machine* in page 296 and log on to each instance of the `elementmanager` VM.
2. Check status of Thinlinc services.

```
service vsmagent status
service vsmserver status
service tlwebaccess status
```

3. If the services are not running, restart them.

   Note: The sequence of restart is important.

```
service vsmagent restart
service vsmserver restart
service tlwebaccess restart
```

Results

Element Manager and Cabinet Viewer opens correctly.

15.2 Element Manager or Cabinet Viewer Launching Error

The following error occurs when launching Element Manager.

"Error initiating the connection to server"

Verify that nslcd service is running on all elementmanager VM's.

Steps

1. Follow the instructions in *Connect to a Virtual Machine* in page 296, then log on to the elementmanager VM.
2. Check the status of service nslcd:

   ```
   service nslcd status
   ```

   If the service nslcd is running the user will see:

   ```
   nslcd (pid  5030) is running...
   ```

   If it is not:

   ```
   nslcd is stopped
   ```

3. If service nslcd is not running on any of elementmanager VM's, start the service:

   ```
   service nslcd start
   ```

   The system will show similar output to:

   ```
   nslcd (pid  5030) is running...
   ```

Results

Element Manager is launched successfully.

15.3 Element Manager or Cabinet Viewer Unavailable in ENM

Element Manager, Cabinet Viewer are not available when you select a node and click on "**Go To**" button.

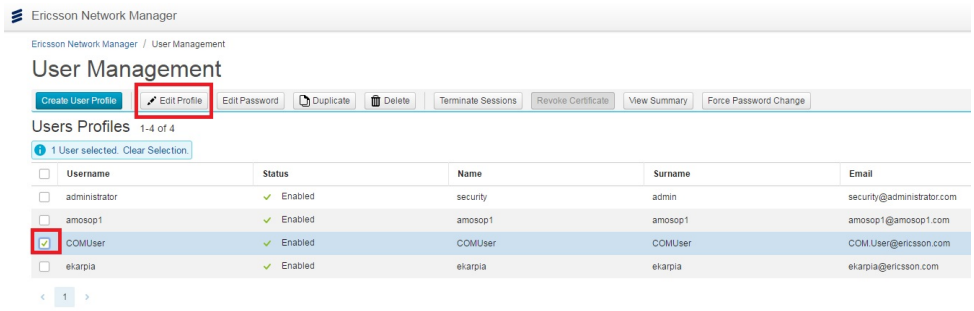
Possible Causes

You do not have the correct roles assigned.

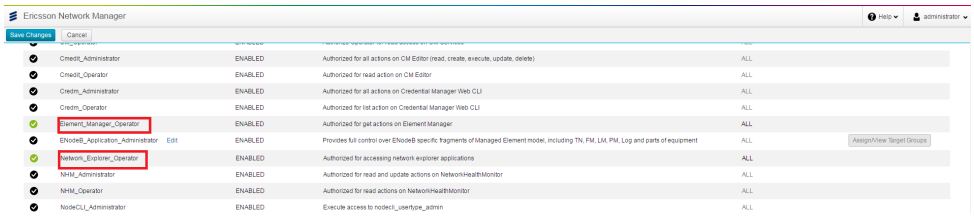
The check this complete the following steps:

Steps

1. Login to ENM as Administrator
2. From the User Management section, select the user, then select **Edit Profile**.



3. Verify that the user has the following roles: Element_Manager_Operator, Network_Explorer_Operator.

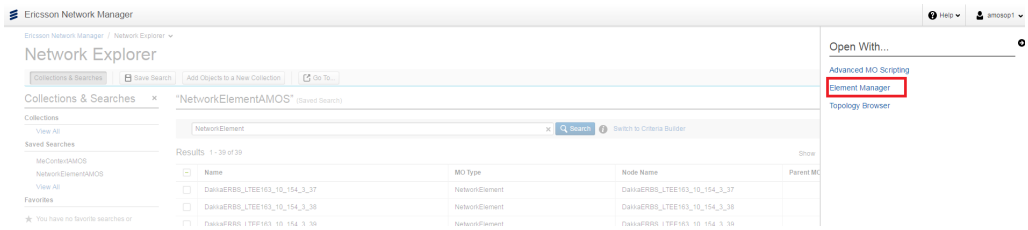


4. If the user does not have both roles, then assign roles to them.

Results

Element Manager is available when you log onto the ENM UI.

Example:



Note: For the **Go To** button to display, a node must be selected from the list.

15.4 Error Launching Element Manager on SL2 Node

When launching Element Manager against an SL2 node, the launch stops and displays a stack trace error.

Cause

The node was previously configured for SL2 on OSS-RC, and the SLS values in the node refer to an unreachable server. The failure to connect to the SLS host is not correctly handled, and the launch fails before attempting to access the local certificate.

Workaround

The SLS values in the node must be cleared to allow correct functioning with ENM.

Prerequisites

— Experience with AMOS.

— Experience with node configuration.

— AMOS Administrator role in ENM.

Steps

1. Launch "*AMOS offline*" from the ENM launcher page to open it against the node, then connect to the node using either the node name or the IP address:

```
OFFLINE> !amos <nodename>
or
OFFLINE> !amos <node.ip.address>
```

2. Check the configuration on the node, the old state of SLS:

```
nodename> cat /c/configuration/sls_address.cfg
```

Note: If this step produces the message: "`File not found: sls_address.cfg`", then SLS configuration is not the problem and this troubleshooting section should be abandoned.

3. Save the old state of SLS to clear the SL2 configuration from the node:

```
nodename> mv /c/configuration/sls_address.cfg /c/configuration/sls_address.c →
fg.old.oss
```

4. If the above procedure needs to be rolled back, copy back the old state of SLS:

```
nodename> mv /c/configuration/sls_address.cfg.old.oss /c/configuration/sls_a →
ddress.cfg
```

Results

Element Manager is launched successfully.

15.5 Install an SIS Server Certificate to Enable Launch of Element Manager from Network Explorer Over HTTPS

> This procedure shows the operator how to install a Site Infrastructure (SIS) server certificate for Session Border Gateway (SBG) on the management host and launch SBG-IS Element Manager. If port 443 is not opened for HTTPS, URL will automatically redirect to HTTP port 80 on the node.

The certificate ensures the operator can launch the **Element Manager** using the HTTPS protocol, after selecting a node for the first time in **Network Explorer**. On completing the procedure, the operator can view the **Integrated Site Management System** welcome page in the **Cendio Thinlinc** desktop.

Prerequisites

The user is assigned one of the following Roles:

— Network_Explorer_Operator.

— Network_Explorer_Administrator and Element_Manager_Operator.

— Element Manager Capabilities.

Steps

1. Select a node in **Network Explorer**.
2. From the **Actions** menu, select **Launch Element Manager**.
3. Choose the action that matches your scenario.

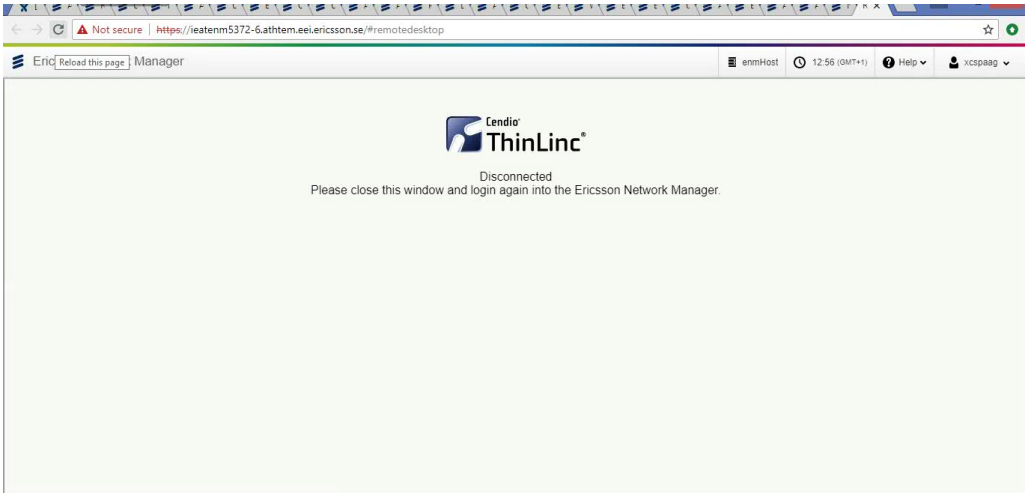
Scenario	Action
I want to use HTTP.	Click **Continue over HTTP**.
I want to use HTTPS. This is the first time I have launched Element Manager over HTTPS for the selected node, so I need to install a certificate.	a. Click **Install Certificate**. b. Select all check boxes in the **Downloading Certificate** popup, and click **OK**. The system installs the SIS server certificate on the management host.
I want to use HTTPS. I have successfully launched Element Manager for the selected node over HTTPS before.	Click **Continue over HTTPS**.

4. Ensure that the **Integrated Site Management System** welcome page now displays. If not, contact Ericsson support.
5. Click **Log In** to provide node credentials.

15.6 Install a Certificate to Launch HLR-FE (IS) Element Manager

Error message while launching Element Manager

When launching Element Manager without a certificate installed, it fails with an error message as follows:



Cause

This is caused by not having a certificate installed.

Workaround

To close unused Cendio Desktops sessions, user may need to contact administrator .

Install an SIS Server Certificate to Enable Launch of Element Manager from Network Explorer Over HTTPS

The certificate lets the operator launch **Element Manager** using the HTTPS protocol, after selecting a node for the first time in **Network Explorer**. On completing the procedure, the operator can view the **Integrated Site Management System** welcome page in the **Cendio Thinlinc** desktop.

Prerequisites

The user is assigned one of the following Roles:

— Network_Explorer_Operator.

— Network_Explorer_Administrator and Element_Manager_Operator.

— Element Manager Capabilities.

Steps

1. Select a node in **Network Explorer**.
2. From the **Actions** menu, select **Launch Element Manager**.

   The **Choose Encryption** page is launched in **Cendio Thinlinc** desktop. The onscreen text indicates that, for first-time use of the HTTPS protocol when launching **Element Manager** for a particular node, a certificate must be installed.
3. Choose the action that matches your scenario.

Scenario	Action
I want to use HTTP.	Click **Continue over HTTP**.
I want to use HTTPS. This is the first time I have launched Element Manager over HTTPS for the selected node, so I need to install a certificate.	a. Click **Install Certificate**. b. Select all check boxes in the **Downloading Certificate** popup, and click **OK**. The system installs the SIS server certificate on the management host.
I want to use HTTPS. I have successfully launched Element Manager for the selected node over HTTPS before.	Click **Continue over HTTPS**.

4. Ensure that the **HLR-FE (IS) (with APG43 Linux)** welcome page is displayed. If it is not, contact Ericsson support.
5. Click **Log In** to provide node credentials.

15.7 Error message while launching Element Manager and Cabinet Viewer

Launch of Element Manager and Cabinet Viewer from Network Explorer fails with an error message as follows:

Cause

This may be caused by the max limit for allowed Cendio Desktop sessions being reached.

The max limit for allowed Cendio Desktop sessions is set to 50 per KVM.

Workaround

To close unused Cendio Desktops sessions, users may need to contact administrator.

Prerequisites

— Element Manager role in ENM

Result

Element Manager and Cabinet Viewer are launched successfully from Network Explorer.

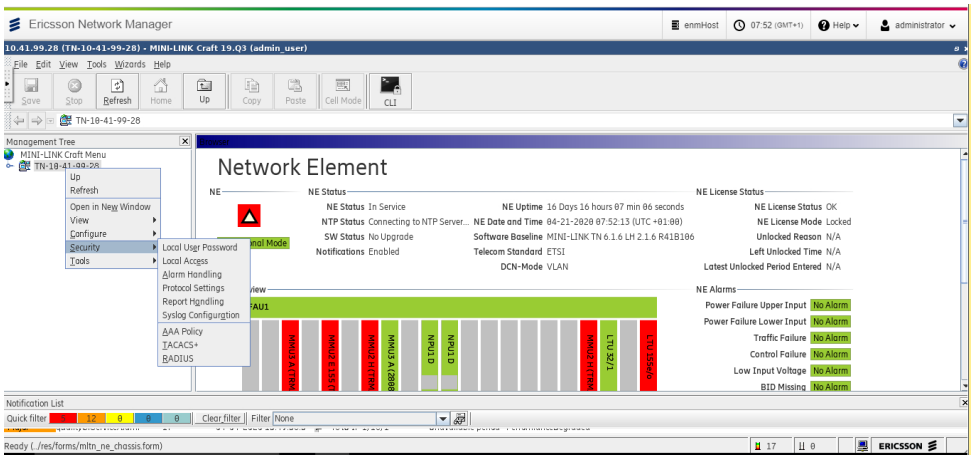
Note: To continue the session once a desktop is available, either enter ENM username and password, or refresh the page.

15.8 Element Manager Launch using TACACS/ RADIUS

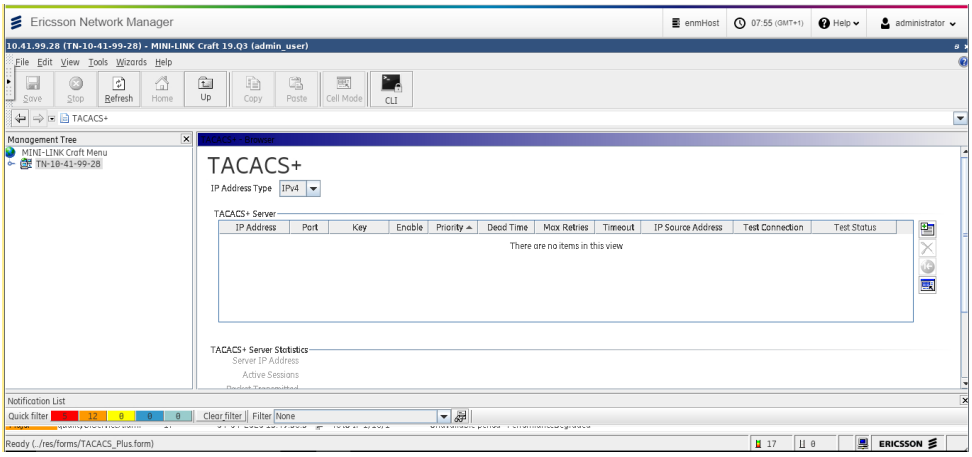
1. Incorrect TACACS/RADIUS configuration.
2. Mismatch between ENM and TACACS+ / RADIUS users.
3. SSO not enabled in ENM.
4. Create mandatory node credentials in TACACS/RADIUS.

Scenario: Element Manager launch failed due to incorrect configuration on TACACS+ / RADIUS

1. To allow SSO from ENM, make sure that the TACACS+/RADIUS server is connected and enabled on the node.
2. The configuration of TACACS+/RADIUS is external to ENM. The TACACS+/RADIUS server must be configured correctly by the security administrator.
3. Launch **Element Manager** with root access and test the enabled and configured TACACS+ / RADIUS connections:



4. Click on **Test Connection** and the status should be connected.



Note: To test RADIUS connection, select **RADIUS** from the menu.

Scenario: Element Manager launch failed due to mismatch between ENM and TACACS+ / RADIUS users

1. ENM user credentials must be available on the TACACS+/RADIUS server.

   Example

   For a user with name `centralized_user1`, the user name and password must be the same on both the TACACS+/RADIUS server and ENM.

Scenario: Element Manager launch failed as SSO is disabled in ENM

1. Check the SSO authentication status in ENM using the `secadm` SSO command.
2. Remote authentication of TACACS/ RADIUS server does not work if SSO is disabled, therefore you must enable SSO.

Scenario: Element Manager launch failed due to node credentials not present on TACACS/RADIUS server

1. Check whether the mandatory node credentials are present on the TACACS +/RADIUS server. Node credentials that are mandatory in ENM while adding a node can be secure user, normal user, root user or nodecli user. These mandatory users are different for each node type.

   For example, if a secure user is mandatory, then secure user credentials must be present in the TACACS+/RADIUS server.

15.9 Unsupported Browser Action Error launching MINI-LINK CRAFT Help/Alarm Description

> After launching Element Manager, in MINI-LINK Craft when we open help options we might encounter the following browser compatibility error:.

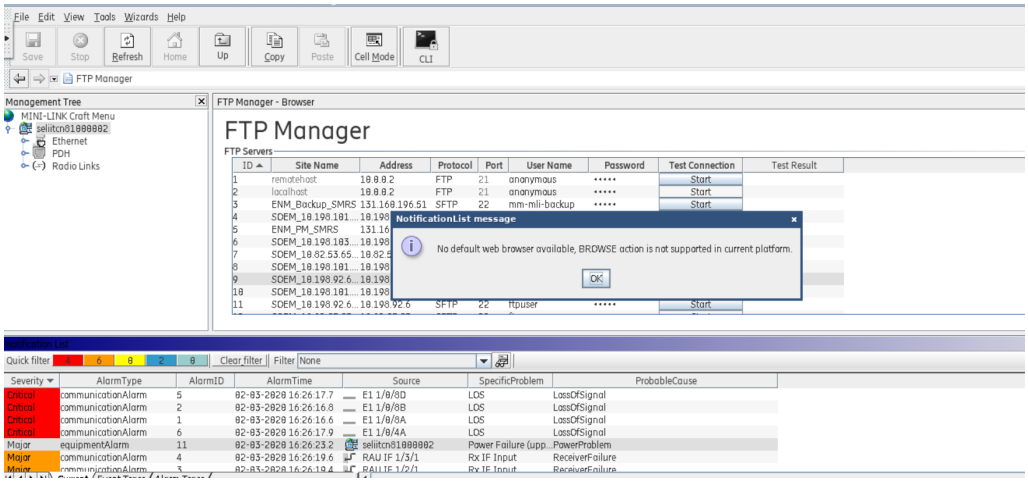


Figure 4 Alarm Description

Solution

1. Open putty and connect to element-manager service group. For example: `[root@cloud-ms-1 ericsson]# ssh -i/root/.ssh/vm_private_key cloud-user@svc-2-elementmanager`
2. sudo su
3. Go to path `cd/opt/ericsson/mlcraft/res/config/`
4. Open XML MLCraft_cfg.env.xml. For example: `viMLCraft_cfg.env.xml`
5. Update the browser path in below line and save with: `!wq:<mlcraft_cfg> <installation_path value="/opt/ericsson/mlcraft"/> <browser_path value="#browser#"/>`For example: `<browser_path value="/usr/bin/firefox"/> </mlcraft_cfg>`
6. Relaunch the Element Manager.

16 Desktop Session Management Troubleshooting Guide

This section provides the troubleshooting steps recommended to diagnose, and fix common problems in the ENM Desktop Session Management.

16.1 Application Launcher is Not Available from ENM UI

The Desktop Session Management link is not available when logged into the ENM UI.

Prerequisites

— User has DesktopSession_Administrator or Administrator role.

Steps

1. Verify that the user has one of the required roles.
2. Log on to the ENM as Administrator, and add the appropriate user role to this user.

16.2 List of Logged Users Not Displayed

ENM Desktop Session Management doesn't display the list of users currently using remote desktop, and their details.

Prerequisites

— Valid user session available for Remote Desktop applications

(eq. Element Manager, Cabinet Viewer and etc).

Steps

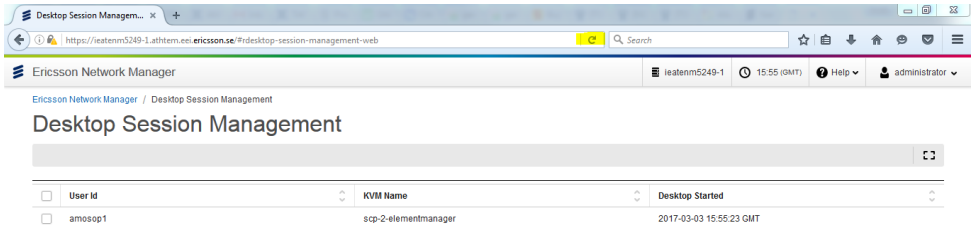
1. Refresh the ENM Desktop Session Management page.

   Example

   Application page before the refresh:

Example

Application page after the refresh:



Results

The list of users with active or valid desktop sessions is displayed.

16.3 Unable to Terminate Active Remote Desktop Sessions

Desktop Session Management displays the error Popup Message "`Failed to delete user(s) session`" when the application is unable to contact the ENM server.

Prerequisites

— User has DesktopSession_Administrator or Administrator to access the application.

— User has LITP Admin access to restart the Element Manager VMs.

Steps

1. Check the network connectivity status.
2. If the application is not connected to the server, restart the Element Manager VMs.

Results

Administrator should be able to terminate any active remote desktop sessions.

17 Release Independence Manager Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in Release Independence Manager.

17.1 Release Independence Script fails during the Model Deployment

If in a row of the Results page corresponding to a Node Version, the status is reported as "failed", and the Node Version is present in the application main page as "Unsupported Version", contact Ericsson Support.

17.2 Resolve Model Download Error

This section describes the steps to resolve Model Download error for a new unsupported node version.

When Release Independence Manager detects a new unsupported node version, the model is downloaded from the node and a full model validation is performed.

If the download fails, Release Independence Manager cannot add support for the unsupported node version. To force the Model Download, a software synchronization of the node is required.

Prerequisites

— Cmedit_Administrator role

Solution

Steps

1. Launch the Command Line Interface (CLI) application from the ENM Launcher.
2. Run a software synchronization command against a node with an unsupported node version where the download failed, specifying the node name.

```
# cmedit action NetworkElement=<NetworkElement_Name> softwareSync
```

Example

```
# cmedit action NetworkElement=LTE95ERBS00001 softwareSync
SUCCESS FDN : NetworkElement=LTE95ERBS00001
```

Note: When the software synchronization command completes, the Model Download error is resolved on Release Independence Manager in timely manner.

Results

The unsupported node version no longer displays the Model Download error.

Note: If the Release Independence Manager still displays the Model Download error, contact Ericsson Support.

17.3 Resolve Model Validation Error

> This section describes the steps recommended to resolve the model validation error for the unsupported Node Version.

When Release Independence Manager automatically detects a new unsupported node version, a full model validation is performed.

If the model validation fails, Release Independence Manager cannot add support for the unsupported Node Version.

Steps

The validation for the new unsupported Node Version failed because of an incompatible model: you can download the validation results from the *Release Independence Manager GUI* and contact Ericsson support to resolve the issue.

17.4 Resolve Node Synchronization Issues after Add Support for Node Versions

This section describes the steps to resolve synchronization issues after the Add Support for Node Versions task has completed, refer to page 296 for more details on the task.

Prerequisites

— Cmedit_Operator role.

— Knowledge of the ENM Command Line Interface, Network Explorer collection concept.

— Knowledge of the Treat As concept.

Steps

1. Check the synchronization status of the Nodes of the new supported Node Version:

   ```
   >> cmedit get <NetworkElement_Name> CmFunction.syncStatus
   ```

   Where `<NetworkElement_Name>` is the name of the node

   Example

   ```
   » cmedit get ERBS-Z7304-103-220 CmFunction.syncStatus
   ```

   Example Command output:

   ```
   FDN : NetworkElement=ERBS-Z7304-103-220,CmFunction=1
   syncStatus : UNSYNCHRONIZED
   ```

2. If the `syncStatus` attribute of the NetworkElement is `UNSYNCHRONIZED`, refer to CM Node Synchronization Troubleshooting - Nodes Supporting ECIM to solve the synchronization issue.
3. If the Node remains unsynchronized and it is required to manage the Node in the new supported version, contact Ericsson Support.
4. To rollback and manage the Nodes in Treat As mode, refer to the *Remove ENM Support For A Node Version* tutorial in the *Release Independence Manager online help*.

Results

The Node is synchronized with the new supported version or synchronized in Treat As mode.

17.5 Apply Attribute Blacklisting procedure to get the Node synchronized

The following procedure shows how to get rid of synchronization issues due to not compatible model attributes. Proceed with attribute blacklisting contacting Ericsson Support for specific action.

Prerequisites

User is confident with Treat As concept.

Steps

The Attribute Blacklisting procedure is an internal procedure to exclude from the node synchronization procedure the not compatible attributes from the new Model, introduced with the new Node Version, to get the nodes synchronized.

Please contact Ericsson Support to proceed further.

Results

The Node is synchronized.

18 Configuration Templates Troubleshooting

18.1 Configuration Templates Link Unavailable from ENM Launcher

The Configuration Templates link is not available when logged into ENM UI.

Steps

1. Verify that the user has either ConfigurationTemplates_Administrator or ConfigurationTemplates_Operator user roles
2. Log on to the ENM as Administrator, then add the appropriate user roles to the user

18.2 Create Button Unavailable from Configuration Templates Page

The Create button is not available in the Configuration Templates page.

Steps

1. Verify that the user has the ConfigurationTemplates_Administrator user role.
2. Log on to the ENM as Administrator, then add the appropriate user role to the user.

18.3 Delete Button Unavailable from Configuration Templates Page

The Delete button is not available in the Configuration Templates page after selecting one or more templates.

Steps

1. Verify that the user has the ConfigurationTemplates_Administrator user role.
2. Log on to the ENM as Administrator, then add the appropriate user role to the user.

18.4 Import Button Unavailable from Configuration Templates Page

The Import button is not available in the Configuration Templates page.

Steps

1. Verify that the user has the ConfigurationTemplates_Administrator role.
2. Log on to the ENM as Administrator, then add the appropriate role to the user.

19 CM CLI Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in the CM CLI.

19.1 CM CLI Commands That Query Too Much Data Generate Error 1042

A command that queries too much data on the CM CLI returns the following error:

```
Error 1042 : Execution Error - Unsupported MO Class in command.
A Network-Wide query for MO Class (<MO Class name>) is performed
 with the executed query, but is not supported, as doing so will
 return an excessive amount of data.
Suggested Solution : Try the command again with 1 or more Nodes
as scope.
```

For each of the following causes of the error message, solutions are described:

- *Cause 1: A GET Command With Unspecified Scope Generates Error 1042* on page 117
- *Cause 2: A Parent-Child GET Command Generates Error 1042* on page 121
- *Cause 3: A SET, ACTION, or DELETE Command Generates Error 1042* on page 124

Cause 1: A GET Command With Unspecified Scope Generates Error 1042

The command has too many results. Blacklists set the maximum allowable results for particular types of GET queries on particular MO Types. The solution involves checking the relevant blacklists, and reducing the scope of the command accordingly.

Solution

1. Identify the blacklist that is applicable to your search, using the examples in the table as a guide.

Example

Table 1

Blacklist	Search Example	Description of Search Example
No attribute or specific attribute criteria	`cmedit get * UtranCell Relation`	Returns all instances of MO Class `UTranCellRelation` in all networks.
	`cmedit get * UtranCell Relation.(loadBalancing,mobilityStatus)`	Returns selected attributes of MO Class `UtranCellRelation` in all networks.
All attribute criteria	`cmedit get * UtranCell Relation.*`	Returns all persistent attributes of MO Class `UtranCellRelation` in all networks.
	`cmedit get * UtranCell Relation.<cm>`	Returns all Configuration Management (CM) attributes of MO Class UtranCellRelation in all networks.

Note: The blacklists, shown in the next step, prevent only network-wide searches (* scope) on listed MO types. Commands using the following are not affected by blacklists:

- Partial or complete node names
- Collections
- Saved searches
- A specified list of Network Elements

2. Identify the maximum number of nodes the GET command can involve for a given MO, so you can reduce the command scope appropriately. Refer to the blacklist you identified in the previous step, which is one of the following:

   - Blacklist - No Attribute or Specific Attribute Criteria
   - Blacklist - All Attribute Criteria

Table 2 Blacklist - No Attribute or Specific Attribute Criteria

MOType	Maximum Number of Nodes Involved in Query
`LoadModule`	`1000`

MOType	Maximum Number of Nodes Involved in Query
SoftwareItem	1000
HwItem	1000
PiuType	1000
ExternalEUtranCellFDD	1000
EUtranCellRelation	1000
ExternalENodeBFunction	10000
UtranCellRelation	5000
TermPointToENB	5000
Hardware	1000
NodeExportResult	100
MeasurementType	100
Slot	1000
GtpuApplicationTunnel	1000
Cdma20001xRttCellRelation	1000
EventType	1000
MeasurementReader	1000
TermPointToLbm	5000
GeranCellRelation	10000
BbLink	5000
SupportedTrackingArea	50
GlobalEnodeb	50
SupportingGlobalEnode	50
GtpPath	5000
FmAlarmType	5000
Schema	10000
PmGroup	15000
OpenAlarm	0
ActivityJob	10000
UtranRelation	1000
FeatureKey	100
CapacityKey	100
OptionalFeatureLicense	1000
FeatureState	100
Rule	1000
SctpAssociation	1000

Table 3 Blacklist - All Attribute Criteria

MOType	Maximum Number of Nodes Involved in Query
LoadModule	100
SoftwareItem	100
HwItem	100
PiuType	1000

MOType	Maximum Number of Nodes Involved in Query
ExternalEUtranCellFDD	100
EUtranCellRelation	100
OptionalFeatureLicense	1000
LicenseUsage	1000
ExternalENodeBFunction	1000
UtranCellRelation	1000
TermPointToENB	1000
ExternalUtranCellFDD	1000
EUtranFreqRelation	1000
UtranFreqRelation	1000
ReliableProgramUniter	10000
Hardware	1000
TermPointToMme	5000
QciProfilePredefined	5000
NodeExportResult	0
EUtranFrequency	1000
MeasurementType	100
Slot	1000
GtpuApplicationTunnel	1000
Cdma20001xRttCellRelation	1000
EventType	100
MeasurementReader	100
TermPointToLbm	5000
GeranCellRelation	1000
BbLink	5000
SupportedTrackingArea	50
GlobalEnodeb	20
SupportingGlobalEnodeb	50
GtpPath	5000
Cdma2000CellRelation	10000
ExternalCdma20001xRttCell	1000
FmAlarmType	1000
Schema	1000
ExternalGeranCell	5000
GeranFrequency	10000
PmGroup	10000
OpenAlarm	0
EUtranCellFDD	1000
EUtranCellTDD	1000
UtranCell	1000
LicenseData	0
ActivityJob	1000
UtranRelation	1000

MOType	Maximum Number of Nodes Involved in Query
FeatureKey	100
CapacityKey	100
OptionalFeatureLicense	100
FeatureState	100
Rule	1000
SctpAssociation	1000

3. Reduce the scope of the command so it involves fewer nodes than **Maximum Number of Nodes Involved in Query**..

Cause 2: A Parent-Child GET Command Generates Error 1042

Parent-child GET commands on the following blacklist of MO Types can involve a maximum of 450 nodes:

- LoadModule
- SoftwareItem
- HwItem
- PiuType
- ExternalEUtranCellFDD
- EUtranCellRelation
- OptionalFeatureLicense
- LicenseUsage
- ExternalENodeBFunction
- UtranCellRelation
- TermPointToENB
- ExternalUtranCellFDD
- EUtranFreqRelation
- UtranFreqRelation
- ReliableProgramUniter
- Hardware

- TermPointToMme
- QciProfilePredefined
- NodeExportResult
- EUtranFrequency
- MeasurementType
- Slot
- GtpuApplicationTunnel
- Cdma20001xRttCellRelation
- EventType
- MeasurementReader
- TermPointToLbm
- GeranCellRelation
- BbLink
- SupportedTrackingArea
- GlobalEnodeb
- SupportingGlobalEnodeb
- GtpPath
- Cdma2000CellRelation
- ExternalCdma20001xRttCell
- FmAlarmType
- Schema
- ExternalGeranCell
- GeranFrequency
- PmGroup
- OpenAlarm
- EUtranCellFDD

- EUtranCellTDD
- UtranCell
- LicenseData
- ActivityJob
- UtranRelation
- FeatureKey
- CapacityKey
- OptionalFeatureLicense
- FeatureState
- Rule
- SctpAssociation

The following are affected by this restriction:

- Collections that contain more than 450 nodes.
- Saved searches that return more than 450 nodes.
- Lists of Network Elements with more than 450 nodes

The following is an example of a parent child search.

Table 4 2

Example Command	Description of Search
`cmedit get LTE32ERBS0* ENodeBFunction ,EUtranCellFDD`	Returns all instances of ENodeBFunction which have a child MO Class instance of EUtranCellFDD for all nodes whose name starts with LTE32ERBS0.

Solution

Reduce the scope of the command so that the search operates on fewer than 450 nodes.

Cause 3: A SET, ACTION, or DELETE Command Generates Error 1042

SET, ACTION, and DELETE commands on MO Types belonging to the following blacklist can involve a maximum of 450 nodes:

- LoadModule
- SoftwareItem
- HwItem
- PiuType
- ExternalEUtranCellFDD
- EUtranCellRelation
- OptionalFeatureLicense
- LicenseUsage
- ExternalENodeBFunction
- UtranCellRelation
- TermPointToENB
- ExternalUtranCellFDD
- EUtranFreqRelation
- UtranFreqRelation
- ReliableProgramUniter
- Hardware
- TermPointToMme
- QciProfilePredefined
- NodeExportResult
- EUtranFrequency
- MeasurementType
- Slot
- GtpuApplicationTunnel
- Cdma20001xRttCellRelation

- EventType
- MeasurementReader
- TermPointToLbm
- GeranCellRelation
- BbLink
- SupportedTrackingArea
- GlobalEnodeb
- SupportingGlobalEnodeb
- GtpPath
- Cdma2000CellRelation
- ExternalCdma20001xRttCell
- FmAlarmType
- Schema
- ExternalGeranCell
- GeranFrequency
- PmGroup
- OpenAlarm
- EUtranCellFDD
- EUtranCellTDD
- UtranCell
- LicenseData
- ActivityJob
- UtranRelation
- FeatureKey
- CapacityKey
- OptionalFeatureLicense
- FeatureState

— Rule

— SctpAssociation

The following are affected by this restriction:

— Collections that contain more than 450 nodes.

— Saved searches that involve more than 450 nodes.

— Lists of Network Elements with more than 450 nodes

The following are example commands:

Table 5

Example Command	Description of Command
`cmedit set LTE32ERBS0* EUtranCellFDD userLabel=newLabel`	Set the userLabel attribute of all instances of EUtranCellFDD for all nodes whose names start with LTE32ERBS0.
`cmedit action LTE32ERBS0* EUtranCellFDD changeFrequency.earfcn=25`	Use the action changeFrequency to change the frequency of all instances of EUtranCellFDD for all nodes whose names start with LTE32ERBS0.
`cmedit delete LTE32ERBS0* EUtranCellFDD --ALL`	Delete all instances of EUtranCellFDD and its children for all nodes whose names start with LTE32ERBS0.

Solution

Reduce the scope of the command so that it operates on fewer than 450 nodes.

19.2 Commands not responding or "hanging"

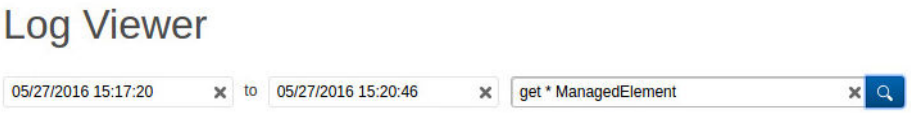
This section describes how to troubleshoot when CM CLI commands do not respond (hang).

Steps

1. Open Log Viewer to view errors logs relating to your command.

   Log Viewer is found in the Application Launcher page under the "System" heading.

   a. In the search criteria text box, enter the time period and (part of) the command that was run (do not include "cmedit") and click **enter**.



If errors are returned for the search criteria, the command has most likely failed. Refresh the CM CLI and rerun the command.

b. If there are no errors in Log Viewer, the command may still be running. Wait until the result is returned, or until the 5 minute timeout is reached.

2. If step 1 was unsuccessful, the CMServ cluster may need to be restarted. To log on to CMServ, refer to the sections *VM Security Tasks* and *Connect to a Virtual Machine* in page 296

   a. ssh onto svc-1

   b. ssh litp-admin@cloud-svc-1 password:

   c. Switch user to root

   ```
   sudo su root
   ```

   d. Check the current state of CMServ cluster on SVC-1 - expecting online

   ```
   hagrp -state | grep _cmserv
   ```

   e. Offline CMServ Cluster on SVC-1

   ```
   hagrp -offline Grp_CS_svc_cluster_cmserv -sys cloud-svc-1
   ```

   f. Check the current state of CMServ cluster on SVC-1 - expecting offline/off lining

   ```
   watch -n1 "hagrp -state | grep _cmserv" - repeats command in quotes
    every second so you don't have to do it manually
   ```

   g. Once CMServ cluster is offline, online in again.

   ```
   hagrp -online Grp_CS_svc_cluster_cmserv cloud-svc-1
   ```

   h. Monitor service group until it is online.

   ```
   watch -n1 "hagrp -state | grep _cmserv"
   ```

   i. Repeat steps e-h for svc-2

When the CMServ clusters are online, rerun the command.

Results

Commands return output.

19.3 HTTP Errors

This section describes some of the common HTTP errors, and possible solutions.

Expected Result

CM CLI will return to normal operation.

HTTP Errors and Possible Solutions

1. HTTP 404 Not Found: This error occurs when there is a connectivity issue between the client and the server.

   Solution: Check if the CMServ cluster is online. Steps to check status and restart the cluster can be found at step 2 of possible solutions on Commands not responding or "hanging" on page 126.

2. HTTP 504 Gateway Timeout: This error occurs when the gateway or proxy does not receive a timely response from the upstream server.

   Solution: The commands being run against the server may be approaching the server capacity.

   If a number of large commands are being run concurrently, wait for commands to return before proceeding. You can also adjust the structure of the command to reduce load on the server.

3. HTTP 500 Internal Server Error: This is displayed when the server has encountered an error, or is not able to perform the request.

   Solution: Restart CMServ cluster if HTTP 500 error code reoccurs. Refer to step 2 of possible solutions on Commands not responding or "hanging" on page 126.

20 Bulk Node CLI Troubleshooting

This section describes the troubleshooting steps recommended to fix error messages when launching Bulk Node CLI.

20.1 Error Message - "User has No Privilege to execute this command"

Cause

The user without administrator rights is importing a blacklist file.

Solution

User must have any one of the following roles assigned to import a blacklist file:

- **Nodecli_system_Administrator**
- **Nodecli_Administrator**
- **Nodecli_Operator**

20.2 Error Message - "Input command list file contains one or more blacklisted commands"

Cause

Bulk node CLI Job is executed with a command list file that contains blacklisted commands.

Solution

Check the commands in the command list file and ensure that the input command list file does not contain any blacklisted commands.

20.3 Error Message - "The JobStatus attribute of the JobDetails is "FAILED"

Cause

Execution of node CLI command has failed or issue with node connectivity.

Solution

Check the `nodecli` logs for node connectivity issues or command execution failures.

20.4 Error Message - "The file commandlistfile1.txt is not attached to command"

Cause

Uploading the `commandlist` file without placing the file in ENM CLI.

Solution

A valid `commandlist` file must be associated with the command. Drag and drop a valid file into the CLI command area.

20.5 Error When Uploading a .cfg File

Cause

Error when uploading a `.cfg` file into the ENM for router nodes.

Solution

— Check if the `smrsserv` service group is online.

— Check if the file system is available on the server.

20.6 Error Message - "Command execution failed (Command execution timed out)"

User must not include commands which require manual intervention in the `commandlist` file.

Cause

Uploading the `commandlist` file with commands which require user intervention.

Solution

Remove commands which require manual intervention from the `commandlist`.
Drag and drop a valid file into the CLI command area.

21 SHM Troubleshooting

This following sections provides procedures and information to diagnose and troubleshoot issues with SHM functionality.

21.1 No Backup Inventory Information Displayed for Selected Nodes

If you encounter problems viewing the backup information for either CPP, ECIM, or GSM(AXE) based nodes, do the steps in following topics to identify and fix these problems.

21.1.1 CPP or ECIM Nodes

The Backup Inventory information for both the CPP and ECIM based nodes is retrieved from the nodes during CM synchronization.

Steps

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the CLI :

   ```
   cmedit get NetworkElement=<networkElement>,CmFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

   The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and the `CmNodeHeartbeatSupervision active` attribute must be `true`.

2. If the `CmFunction syncStatus` is `UNSYNCHRONIZED` and `CmNodeHeartbeatSupervision active` is false, change `CmNodeHeartbeatSupervision active` to `true`:

   ```
   cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
   ve=true
   ```

   Note: Note - It may take a few seconds for the `CmFunction syncStatus` attribute value to change to `SYNCHRONIZED`. When the node is in `SYNCHRONIZED`, the backup inventory is displayed.

3. If the `CmFunction syncStatus` attribute remains `UNSYNCHRONIZED`, perform a manual sync:

   ```
   cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
   ```

4. If no backup information is displayed after performing the manual sync and the CmFunction syncStatus attribute remains UNSYNCHRONIZED, contact Ericsson support for further assistance.

21.1.2 GSM (AXE) Nodes

For AXE nodes, inventory data is retrieved from the nodes during Inventory synchronization.

Steps

1. Check the value of the InventoryFunction syncStatus attribute and the value of the InventorySupervision active attribute using the CLI:

```
cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
```

```
cmedit get NetworkElement=<networkElement>,InventorySupervision=1
```

   The InventoryFunction syncStatus attribute must be SYNCHRONIZED and the InventorySupervision attribute must be true.

2. If the InventoryFunction syncStatus attribute is UNSYNCHRONIZED and InventorySupervision active is false, set InventorySupervision active to true:

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

   If the InventoryFunction syncStatus changes to SYNCHRONIZED, the AXE backup inventory information is displayed.

   Note: It may take a few seconds for the InventoryFunction syncStatus attribute value to change to SYNCHRONIZED.

3. If the InventoryFunction syncStatus attribute remains UNSYNCHRONIZED and no backup inventory information is displayed, do a manual sync.

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize
```

   If the InventoryFunction syncStatus changes to SYNCHRONIZED, the AXE backup inventory information is displayed.

   Note: It may take a few seconds for the InventoryFunction syncStatus attribute value to change to SYNCHRONIZED.

4. If no backup information is displayed after performing the manual sync, contact Ericsson support for further assistance. Before contacting Ericsson

support, check if the `InventoryFunction syncStatus` is `SYNCHRONIZED`. If yes, run the following command and collect the output.

```
cmedit get <nodename> BackUpInventory.*
```

Example

```
cmedit get MSC02BSC03 BackUpInventory.*
FDN : SubNetwork=NETSimG,MeContext=MSC02BSC03,Inventory=1,BackupInventory=1
brmBackupManagerId : 1
component : null
createdBy : null
domain : null
lastSuccessfulSynchTime : Wed Mar 13 10:15:44 GMT 2019
type : null
```

5. If backup information is displayed after selecting a node and no information is displayed after clicking **View Backup Items**, then the node may not have second-level inventory.

```
cmedit get <nodename> BackUpItem.*
```

Example

```
cmedit get MSC02BSC03 BackUpItem.*
FDN : SubNetwork=NETSimG,MeContext=MSC02BSC03,Inventory=1,BackupInventory=1, →
BackupItem=1
comments : null
component : APG1
creationTime : Thu Jan 31 16:13:00 GMT 2019
domain : BRM_SYSTEM_DATA
id : 1
name : BSC015-43L-3_5_0-R6A-2019-01-31T16-13-23
status : null
type : BRM_SYSTEM_DATA
userLabel : null
```

If second-level inventory details are shown in the output, then collect the output and contact Ericsson Support.

21.2 Troubleshoot Backup Jobs

In SHM, the Backup Job creates a backup of the node software and configuration. The backup is used to rollback a node a previous configuration (for example, in the event of failure or if you encounter an issue with the current software and configuration) .

The following table lists error scenarios that may occur while creating a Backup Job. The table also lists the related failure message displayed in the *Job Logs* page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
Backup Job Fails on the Selected Nodes with Job Logs Message - "Node is not in sync with ENM"	For the Backup Job to be successful, the nodes must be synchronized with ENM.

Scenario	Comment
Backup Job Fails on the Selected Nodes with Job Logs Message - "Creation of CV Failed"	If the number of backups on a node exceeds the defined limit, the backup cannot be created. Verify if the number of backups on the node exceeds the maximum value, delete the oldest backup and create the backup job again.
Backup Job Fails on the Selected Nodes with Job Logs Message - "Upload Configuration Version activity failed with reason 1 : FTP server is not accessible."	Check the SFTP connection between ENM and Node.

21.2.1 Scenario: Backup Job Fails on the Selected Nodes with Job Logs Message - "Node is not in sync with ENM"

For a Backup Job to be successful, the nodes must be synchronized with ENM. For CPP and ECIM nodes run the following steps.

Steps

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the ENM CLI :

   ```
   cmedit get NetworkElement=<networkElement>,CmFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

   The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and and the `CmNodeHeartbeatSupervision active` attribute must be `true`.

2. If the `CmFunction syncStatus` is `UNSYNCHRONIZED` and `CmNodeHeartbeatSupervision active` is false, change `CmNodeHeartbeatSupervision active` to `true`:

   ```
   cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
   ve=true
   ```

   Note: It may take a few seconds for the `CmFunction syncStatus` attribute value to change to `SYNCHRONIZED`. When the node is `SYNCHRONIZED`, create the backup job again.

3. If the `CmFunction syncStatus` attribute remains `UNSYNCHRONIZED`, perform a manual sync:

   ```
   cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
   ```

   If the `CmFunction syncStatus` attribute value remains `UNSYNCHRONIZED` contact Ericsson support for further assistance.

21.2.2 Scenario: Backup Job Fails on the Selected Nodes with Job Logs Message - "Creation of CV Failed"

If the number of backups on a node exceeds the specified limit, the backup cannot be created. Check if the number of backups on the node exceeds the limit, delete the oldest backup, and re-create the backup job.

The following procedures describe how to troubleshoot this scenario for ECIM and CPP nodes.

21.2.2.1 ECIM Nodes

1. On an ECIM node, the `maxStoredManualBackups` attribute on the `BrmBackupHousekeeping` MO defines the maximum number of backups for that node. Retrieve the `Brmbackupmanager` FDN and check the `BrmBackupHousekeeping` value.

   Example

   ```
   cmedit get <networkElement> Brmbackupmanager
   Example:
   cmedit get LTE01dg2ERBS00003 BrmBackupManager
   Response:
   FDN: ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,Brm=1,BrmBackupmanag →
   er=1
   ```

   Example

   ```
   cmedit get <FDN>,BrmBackupHousekeeping.*
   Example:
   cmedit get ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,Brm=1,BrmBacku →
   pmanager=1,BrmBackupHousekeeping.*
   Response:
   FDN: ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,Brm=1,BrmBackupmanag →
   er=1,BrmBackupHousekeeping=1
   autoDelete : ENABLED
   brmBackupHousekeepingId : 1
   maxStoredManualBackups : 20
   ```

2. In the SHM UI, launch the Backup Administration page and add the relevant ECIM node using **Network** > **Add Topology Data** drop-down.

   The Backups table lists all the backups that exist for this node. The column Location indicates if the backup is stored on the NODE or in ENM.

3. Check the total number of backups stored on the node (Location is NODE).

4. If the number of backups on the node equals the `maxStoredManualBackups` value (for example, `maxStoredManualBackups : 20`), delete the oldest backup by creating and executing a Delete Backup Job.

5. Once the backup is successfully deleted, create a backup job on the node again.

21.2.2.2 CPP Nodes

The maximum number of backups that can be stored on a CPP node is 50. This value is not configurable.

Steps

1. In the SHM UI, launch the Backup Administration page and add the relevant CPP node using **Network** > **Add Topology Data** drop-down.

   The Backups table lists all the backups that exist for this node. The column Location indicates if the backup is stored on the NODE or in ENM.

2. Check the total number of backups stored on the Node (Location is NODE).

3. If the number of backups on the node is equal to 50, delete the oldest backup by creating a Delete Backup Job.

4. Once the backup is successfully deleted, create a backup job on the node again.

21.2.3 Scenario: Backup Job Fails on the Selected Nodes with Job Logs Message - "Upload Configuration Version activity failed with reason "1" : "FTP server is not accessible."

For the Backup Job upload activity to be successful the SFTP connection between ENM and Node must be working. For CPP and ECIM nodes run the following steps.

Steps

1. Ensure that the SFTP connection is enabled on the node and the PORT is open.

   Refer to page 296.

2. Create the Backup Job again once the connection is established between ENM and Node.

After This Task

If none of the troubleshooting steps resolves the issue, contact Ericsson support for further assistance.

21.3 No Hardware Inventory Information Displayed for Selected Nodes

In SHM, the Hardware Administration functionality displays hardware inventory information about the supported nodes in your network. If you encounter

problems viewing the hardware information in the Hardware Administration page, perform the steps in this topic to identify and fix these problems.

— For CPP nodes, inventory data is retrieved from the nodes during Inventory synchronization.

— For ECIM nodes, inventory data is retrieved from the nodes during CM synchronization.

— For AXE nodes, inventory data is retrieved from the nodes during Inventory synchronization.

21.3.1 CPP Nodes

1. Check the value of the `InventoryFunction syncStatus` attribute and the value of the `InventorySupervision active` attribute using the ENM CLI.

```
cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
```

```
cmedit get NetworkElement=<networkElement>,InventorySupervision=1
```

   The `InventoryFunction syncStatus` must be `SYNCHRONIZED` and `InventorySupervision active` must be `true`.

2. If the `InventoryFunction syncStatus` attribute is `UNSYNCHRONIZED` and the `InventorySupervision active` attribute is `false`, set `InventorySupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

   If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the CPP hardware inventory information should now be displayed.

   Note: `InventoryFunction syncStatusIt may take a few seconds for the` attribute value to change to `SYNCHRONIZED`.

3. If the `InventoryFunction syncStatus` remains `UNSYNCHRONIZED` (and no hardware information is displayed), perform a manual sync.

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize.(invType=ALL)
```

   If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the CPP hardware inventory information should now be displayed.

   Note: It may take a few seconds for the `InventoryFunction syncStatus` attribute value to change to `SYNCHRONIZED`.

4. If no hardware information is displayed after performing the manual sync, contact Ericsson support.

   Before contacting Ericsson support, check if the `InventoryFunction syncStatus` is `SYNCHRONIZED`. If so, run the following command and collect the output.

   ```
   cmedit get <FDN>,Inventory=1,HWInventory=1
   ```

5. If hardware information is displayed after selecting a node and no information is displayed after clicking **View Hardware Items** then the node may not have second level inventory.

   Run the following command to verify:

   ```
   cmedit get <nodename> Hardware.*
   ```

   In the command output, `Elements` with `slotNumber(slotNo)`other than `0` or `Elements` with `productName` containing `FAN` or `PFM` or `O/E` corresponds to second level inventory.

   ```
   cmedit get ieatnetsimv7039-33_LTE03ERBS00001 Hardware.*
   FDN : SubNetwork=ERBS-SUBNW-1,MeContext=ieatnetsimv7039-33_LTE03ERBS00001,Inventory=1,H →
   WInventory=1,Hardware=8
   hardwareId : 8
   hwPos : {slotNo=7, subrackId=}
   noOfSlots : null
   productData : {productNumber=ENM14B, productDate=null, productName=ERBS14B, productRevi →
   sion=7CXP324}
   serialNo : 3oQ
   ```

   If second level inventory details are shown in the output, then collect the output and contact Ericsson Support.

21.3.2 ECIM Nodes

Note: For SGSN-MME nodes, there is no second level inventory, only the first level hardware inventory information is displayed on the Hardware Administration page

Steps

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervisionactive` attribute using the CLI .

   ```
   cmedit get NetworkElement=<networkElement>, CmFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

   The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and and the `CmNodeHeartbeatSupervisionactive` attribute must be `true`.

2. If the CmFunction syncStatus is UNSYNCHRONIZED and CmNodeHeartbeatSupervisionactive is false, change CmNodeHeartbeatSupervisionactive to true.

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

   If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM hardware information should now be displayed.

   Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

3. If the CmFunction syncStatus attribute remains UNSYNCHRONIZED (and no hardware information is displayed), perform a manual sync.

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

   If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM hardware information should now be displayed.

   Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

4. If no hardware information is displayed after performing the manual sync, contact Ericsson support.

   Before contacting Ericsson support, check if the CmFunction syncStatus is SYNCHRONIZED. If so, execute the following command and collect the output.

```
cmedit get <FDN>,SystemFunctions=1,HwInventory=1,HwItem=1
```

5. If hardware information is displayed after selecting a node and no information is displayed after clicking **View Hardware Items** then the node may not have second level inventory.

   Run the following CLI command to verify:

```
cmedit get <nodename> HwItem
```

   In the command output, the FDNs ending with HwItem=[Int],HwItem=[Int] corresponds to second level inventory.

```
cmedit get LTE01dg2ERBS00003 HwItem
FDN : SubNetwork=NETSimW,ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,HwInventory →
=1,HwItem=1
FDN : SubNetwork=NETSimW,ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,HwInventory →
=1,HwItem=1,HwItem=1
FDN : SubNetwork=NETSimW,ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,HwInventory →
=1,HwItem=15237987997195
```

If the second level inventory details are shown in the output, then collect the output and contact Ericsson Support.

21.3.3 AXE Nodes

Steps

1. Check the value of the `InventoryFunction syncStatus` and `InventorySupervision active` attribute using the ENM CLI.

```
cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
```

```
cmedit get NetworkElement=<networkElement>,InventorySupervision=1
```

   The `InventoryFunction syncStatus` must be `SYNCHRONIZED` and the `InventorySupervision active` must be `true`.

2. If the `InventoryFunction syncStatus` attribute is `UNSYNCHRONIZED` and `InventorySupervision active` attribute is `false`, set `InventorySupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

   If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the AXE hardware information is displayed.

   Note: It may take a few minutes for the `InventoryFunction syncStatus` to change to `SYNCHRONIZED`.

3. If the `InventoryFunction syncStatus` remains `UNSYNCHRONIZED` and no hardware information is displayed, do a manual sync.

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize
```

   If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the AXE hardware inventory information is displayed.

   Note: It may take a few minutes for the `InventoryFunction syncStatus` to change to `SYNCHRONIZED`.

4. If no hardware information is displayed after performing the manual sync, contact Ericsson support.

   Before contacting Ericsson support, check if the `InventoryFunction syncStatus` is `SYNCHRONIZED`. If yes, run the following command and collect the output.

```
cmedit get <FDN>,Inventory=1,HardwareInventory=1
```

5. If hardware information is displayed after selecting a node and no information is displayed after clicking **View Hardware Items**, then the node may not have second level inventory.

   Run the following CLI command to verify:

   ```
   cmedit get <nodename> HardwareShelf.*
   ```

   Example

   ```
   # cmedit get MSC06 HardwareShelf.*
   ```

   ```
   FDN : MeContext=MSC06,Inventory=1,HardwareInventory=1,HardwareShelf=1
   hardwareType : Shelf
   id : 1
   noOfBoards : 11
   shelfId : 0.0.0.0.
   unitLocation : Address plug0=0,Address plug1=0,Address plug2=0,Address plug3=0
   ```

   First-level data is shown in the CLI.

   On runnng the following command, second-level data is shown in the CLI.

   ```
   cmedit get <nodename> HardwareBlade.*
   ```

   Example

   ```
   # cmedit get MSC06 HardwareBlade.*
   ```

   ```
   FDN : MeContext=MSC06,Inventory=1,HardwareInventory=1,HardwareBlade=2
   administrativeData : {productNumber=ROJ 208 866/5, productName=GEP5-64, productRevision →
   =R2C}
   bladeExecutionSide : A
   boardName : CPUB
   hardwaretype : CP
   id : 2
   serialNumber : null
   unitLocation : 1
   vendor : null
   ```

   If the second-level inventory details are shown in the output, then collect the output and contact Ericsson Support.

21.4 Troubleshoot Install License Key Jobs

In SHM, the License Job installs the selected key files on the node. License Installation enables certain features and capacity on the node.

The following table lists error scenarios that can occur while executing a License Job. The table also lists the related failure message displayed in the Job Logs

page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
Install License Job Fails on the Selected nodes with Job Logs Message - "Precheck for Install License Key File is failed. Reason: Licensing MO not found". on page 143	If Install License Key File precheck fails and the License MO is not present, the license job cannot be created. Check if the node has been deleted. For the License Job to be successful, the nodes must be synchronized with ENM.
Install License Job Fails on the Selected Nodes with Job Logs Message - "License Key file not found." on page 144	If the license key file is not present, the license job cannot be created. Verify that the corresponding license key file exists.
License Inventory Update Issue after Install License Job for R6000 Nodes on page 145	For R6000 nodes, after a license installation job is successful, the update of the License Key File MOs on the node takes around 15 minutes. The linked-to procedure shows how to complete this task immediately.
Install License Job Created from ASU/CLI Is Skipped on the Selected Nodes with Job Logs Message - "License Key File Not Found" on page 145	If the license key file is not present or is already installed, the license job is skipped. Import the latest license key file and create an install license job.

21.4.1 Install License Job Fails on the Selected nodes with Job Logs Message - "Precheck for Install License Key File is failed. Reason: Licensing MO not found".

> This scenario can occur if the node is not synchronized with ENM or if the node is deleted before the Install License Job executes (for example, if the install job execution is scheduled for a future date).

To resolve these issues, execute the following steps for the CPP and ECIM based nodes:

Steps

1. Check if the node has been deleted.

   ```
   cmedit get NetworkElement=<networkElement>
   ```

   A response of `0 instance(s)` indicates the node has been deleted.

2. If the node has not been deleted check the node synchronization status.

3. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the CLI

   ```
   cmedit get NetworkElement=<networkElement>, CmFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

   The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and and the `CmNodeHeartbeatSupervision active` attribute must be `true`.

4. If the `CmFunction syncStatus` is `UNSYNCHRONIZED` and `CmNodeHeartbeatSupervision active` is false, change `CmNodeHeartbeatSupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

   Note: It may take a few seconds for the `CmFunction syncStatus` to change to `SYNCHRONIZED`.

5. If the `CmFunction syncStatus` attribute remains `UNSYNCHRONIZED`, execute the following manual sync command:

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

   Note: It may take a few seconds for the `CmFunction syncStatus` to change to `SYNCHRONIZED`.

6. If the `CmFunction syncStatus` attribute remains `UNSYNCHRONIZED`, then contact Ericsson support for further assistance.

21.4.2 Install License Job Fails on the Selected Nodes with Job Logs Message - "License Key file not found."

For a License Job to be successful, the License Key file must be present in ENM. To check if corresponding License Key file exists, execute the following steps for the CPP & ECIM based nodes:

Steps

1. In the SHM UI, launch the License Administration page and select View Imported Key Files .
2. The Imported Key Files table displays the list of all imported key files.
3. If the required key file is not displayed in the table, import the key file into ENM (using Import Key Files).
4. Create the Install License job again on the node.
5. If these steps do not resolve the issues, contact Ericsson support for further assistance.

21.4.3 License Inventory Update Issue after Install License Job for R6000 Nodes

> How to immediately update License Key File MOs on node after license installation job is successful.

For R6000 nodes, after a license installation job is successful, the update of the License Key File MOs on the node will take around 15 minutes.

To update the license MOs immediately, and reflect the same in ENM license inventory, perform the following steps:

Steps

1. Execute the following commands on node:
    a. `[local]Ericsson#licensing inventory refresh`
    b. `[local]Ericsson#licensing inventory publish`
2. Synchronize the node manually to get the updated license inventory in ENM:
    a. Manually sync the node in ENM

    ```
    cmedit action NetworkElement=<NodeName>,CmFunction=1
    sync
    ```

    b. Check the sync status of the node in ENM

    ```
    cmedit get NetworkElement=<NodeName>,CmFunction=1
    ```

21.4.4 Install License Job Created from ASU/CLI Is Skipped on the Selected Nodes with Job Logs Message - "License Key File Not Found"

For a License Job to be successful, the License Key File must be present in ENM. To check if corresponding License Key File exists, execute the following steps for the CPP-based nodes and for ECIM-based nodes:

Steps

1. In the SHM UI, launch the **License Administration** page and select **View Imported Key Files** .

    The **Imported Key Files** table lists all imported key files.
2. Import the key file into ENM (using **Import Key Files**), if the needed key file is not displayed in the table.
3. Create the **Install License** job again on the node.

4. Contact Ericsson support for further assistance, if these steps do not resolve the issues.

21.5 No License Inventory Information Displayed for Selected Nodes

In SHM, the License Administration functionality displays license information about the nodes in your network. If you encounter problems viewing the license information in the *License Administration* page perform the steps in this topic to identify and fix these problems.

SHM does not support/provide License Inventory information for all nodes. In the *License Administration* page Network panel, an information icon is displayed beside the unsupported nodes with the note "`Inventory is not supported for this node`". SHM does not display License Inventory information for these unsupported nodes.

For supported nodes, if SHM does not display Inventory Information in the *License Administration* page check the node synchronization status using Command Line Interface application.

— For the CPP based nodes, inventory data is retrieved from the nodes during Inventory synchronization.

— For the ECIM nodes, inventory data is retrieved from the nodes during CM synchronization.

21.5.1 Troubleshooting Steps for CPP based Nodes

1. Check the value of the `InventoryFunction syncStatus` attribute and the value of the `InventorySupervision active` attribute using the ENM CLI

```
cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
```

```
cmedit get NetworkElement=<networkElement>,InventorySupervision=1
```

   The `InventoryFunction syncStatus` must be `SYNCHRONIZED` and *InventorySupervision active* must be `true`.

2. If the `InventoryFunction syncStatus` attribute is `UNSYNCHRONIZED` and the `InventorySupervision active` attribute is `false`, set `InventorySupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

   If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the CPP license inventory information should be displayed.

Note: It may take a few seconds for the InventoryFunction syncStatus attribute value to change to SYNCHRONIZED.

3. If the InventoryFunction syncStatus remains UNSYNCHRONIZED (and no license information is displayed) perform a manual sync:

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize.(invType=ALL)
```

If the InventoryFunction syncStatus changes to SYNCHRONIZED, the CPP license inventory information should be displayed.

Note: It may take a few seconds for the InventoryFunction syncStatus attribute value to change to SYNCHRONIZED.

4. If no license information is displayed after performing the manual sync contact Ericsson support.

Before contacting Ericsson support, check if the InventoryFunction syncStatus is SYNCHRONIZED. If it is, run the following command and collect the output.

```
cmedit get <FDN>,Inventory=1,LicenseInventory=1
```

21.5.2 Troubleshooting Steps for ECIM Nodes

Note: For SGSN-MME nodes, as there is no license support, license inventory is not displayed on the License Administration page

Steps

1. Check the value of the CmFunction syncStatus attribute and the value of the CmNodeHeartbeatSupervision active attribute using the CLI :

```
cmedit get NetworkElement=<networkElement>,CmFunction=1
```

```
cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
```

The CmFunction syncStatus attribute must be SYNCHRONIZED and and the CmNodeHeartbeatSupervision active attribute must be true.

2. If the CmFunction syncStatus is UNSYNCHRONIZED and CmNodeHeartbeatSupervision active is false, change CmNodeHeartbeatSupervision active to true:

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM license information should be displayed.

Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

3. If the CmFunction syncStatus attribute remains UNSYNCHRONIZED (and no license information is displayed), perform a manual sync:

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM license information should be displayed.

Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

4. If no license information is displayed after performing the manual sync contact Ericsson support.

Before contacting Ericsson support, check if the CmFunction syncStatus is SYNCHRONIZED. If it is, run the following command and collect the output.

```
cmedit get <FDN>,SystemFunctions=1,Lm=1,KeyFileManagement=1,KeyFileInformati →
on=1
```

21.6 Troubleshoot Restore Jobs

In SHM, the Restore Job enables you to restore the node to a configuration defined in a previously created backup. The restore activities differ for CPP and ECIM based nodes.

The following table lists error scenarios that may occur while executing the Restore Job. The table also lists the related failure message displayed in the Job Logs page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
Restore Job Fails on CPP based Nodes with Job Logs Message - "Unable to proceed Install activity because MO current state is not supported"	The Install activity cannot proceed if the state attribute on the UpgradePackage MO has any of the following values: — UPGRADE_EXECUTING — AWAITING_CONFIRMATION — ONLY_DELETEABLE — INSTALL_EXECUTING
Restore Job Fails on CPP based Nodes with Job Logs Message - "Unable to proceed Install activity because software packages are not available for <product number>:<product revision> in ENM"	The Install activity replaces corrupted upgrade packages that are identified in the verification activity in restore job. For this, the required software packages must be available in ENM.

Scenario	Comment
Restore Job Fails on ECIM based Nodes with Job Logs Message - "Backup File <BackupfileName> doesn't exist on node to restore"	This issue occurs if the required backup file does not exist on the node or has been deleted in a job defined for scheduled or manual execution.
Restore Job Fails on ECIM based nodes with Job Logs Message - "Unable to proceed Confirm Backup activity because Last restored backup value is not set in BrmBackupLabelStore MO for the node <NodeName>"	For the Confirm activity in restore job to be successful, the `lastRestoredbackup` attribute on the `BrmBackupLabelStore` MO must be same as the name of the backup being confirmed to restore.

21.6.1 Scenario - Restore Job Fails on CPP based Nodes with Job Logs Message - "Unable to proceed Install activity because MO current state is not supported"

To check the upgrade package state on the MO, perform the following steps.

Steps

1. Check for state attribute from the `UpgradePackage` MO using the command in ENM CLI:

   ```
   cmedit get <NetworkElement> UpgradePackage.*
   ```

2. If the state attribute is one of the following the job execution does not proceed:

   - `UPGRADE_EXECUTING`
   - `AWAITING_CONFIRMATION`
   - `ONLY_DELETEABLE`
   - `INSTALL_EXECUTING`

21.6.2 Scenario - Restore Job Fails on CPP based Nodes with Job Logs Message - "Unable to proceed Install activity because software packages are not available for <product number>:<product revision> in ENM"

When `Install` activity is selected in the restore job, the `Verify` activity is also selected to execute on the node. The `Install` activity replaces any missing or corrupted upgrade packages that are identified in the `Verify` activity. The software packages identified to be installed must be available in ENM.

Steps

1. In the SHM UI, launch the Software Administration page. Click **View Software Packages** link in quick action bar.

   The Software Packages table displays a list of all the imported software packages.

2. If the required package is not listed, you need to import the software package into ENM.
3. In the Software Administration page, click **Import Software Package** to import the required package.
4. Create the restore job again on the node.

21.6.3 Scenario - Restore Job Fails on ECIM based Nodes with Job Logs Message - "Backup File <BackupfileName> doesn't exist on node to restore"

This issue occurs if the backup file selected to restore the node does not exist on the node or has been deleted in a job defined for scheduled or manual execution.

Steps

1. Check the BrmBackup MO using the following command:

```
cmedit get <NetworkElement> BrmBackup.*
```

2. In the response obtained, check the `backupName` attribute value for the backup name selected in the job.
3. If it does not exist, that means backup is not present on the node. Create the restore job again with a different backup.

   Note: Before triggering Restore activity, ensure that Download and Verify activities are completed in a Restore Job.

21.6.4 Scenario - Restore Job fails on ECIM based nodes with Job Logs Message - "Unable to proceed Confirm Backup activity because Last restored backup value is not set in BrmBackupLabelStore MO for the node <NodeName>"

For the `Confirm` activity in restore job to be successful, the `lastRestoredbackup` attribute on the `BrmBackupLabelStore` MO must be same as the name of the backup being confirmed to restore.

Steps

1. Retrieve BrmBackupLabelStore MO using the following command:

```
cmedit get <NodeName> BrmBackupLabelStore.lastRestoredbackup
```

   Example

```
cmedit get SGSN-16A-CP01-V102 BrmBackupLabelStore.lastRestoredbackup

FDN : SubNetwork=subnet_SGSN-16A-CP01-V102,MeContext=SGSN-16A-CP01-V102,Mana →
gedElement=SGSN-16A-CP01-V102,SystemFunctions=1,BrM=1,BrmBackupManager=1,Brm →
```

```
BackupLabelStore=1
lastRestoredBackup : SGSN-16A-CP01-V102_Restored
```

2. In the response, check `lastRestoredbackup` attribute.

   If the value is not same as the name of backup selected to restore, that means, backup is not restored on node.

3. Create the Restore Job again by selecting all the activities.

After This Task

If none of the troubleshooting steps resolves the issue, contact Ericsson support for further assistance.

21.7 No Software Inventory Information Displayed for Selected Nodes

In SHM, the Software Administration functionality displays the information about the active software running on the nodes in your network. If you encounter problems viewing the software inventory information in the *Software Administration* page, perform the steps in this topic to identify and fix these problems.

— For CPP nodes, inventory data is retrieved from the nodes during Inventory synchronization.

— For ECIM nodes, inventory data is retrieved from the nodes during CM synchronization.

— For AXE nodes, inventory data is retrieved from the nodes during Inventory synchronization.

21.7.1 Troubleshooting Steps for CPP Nodes

1. Check the value of the `InventoryFunction syncStatus` attribute and the value of the `InventorySupervision active` attribute using the ENM CLI.

   ```
   cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,InventorySupervision=1
   ```

   The `InventoryFunction syncStatus` must be `SYNCHRONIZED` and `InventorySupervision active` must be `true`.

2. If the `InventoryFunction syncStatus` attribute is `UNSYNCHRONIZED` and the `InventorySupervision active` attribute is `false`, set `InventorySupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the CPP software inventory information should be displayed.

Note: It may take a few seconds for the `InventoryFunction syncStatus` attribute value to change to `SYNCHRONIZED`.

3. If the `InventoryFunction syncStatus` remains `UNSYNCHRONIZED` (and no software information is displayed), perform a manual sync.

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize.(invType=ALL)
```

If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the CPP software inventory information should be displayed.

Note: It may take a few seconds for the `InventoryFunction syncStatus` attribute value to change to `SYNCHRONIZED`.

4. If no software information is displayed after performing the manual sync, contact Ericsson support.

   Before contacting Ericsson support, check if the `InventoryFunction syncStatus` is `SYNCHRONIZED`. If it is, run the following command and collect the output.

```
cmedit get <FDN>,Inventory=1,SWInventory=1
```

21.7.2 Troubleshooting Steps for ECIM Nodes

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the CLI.

```
cmedit get NetworkElement=<networkElement>, CmFunction=1
```

```
cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
```

   Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the CLI.

2. If the `CmFunction syncStatus` is `UNSYNCHRONIZED` and `CmNodeHeartbeatSupervision active` is false, change `CmNodeHeartbeatSupervision active` to `true`.

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM software information should be displayed.

Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

3. If the CmFunction syncStatus attribute remains UNSYNCHRONIZED (and no software information is displayed), perform a manual sync:

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

If the CmFunction syncStatus changes to SYNCHRONIZED, the ECIM software information should be displayed.

Note: It may take a few seconds for the CmFunction syncStatus to change to SYNCHRONIZED.

4. If no software information is displayed after performing the manual sync, contact Ericsson support.

Before contacting Ericsson support, check if the CmFunction syncStatus is SYNCHRONIZED. If so, execute the following command and collect the output.

```
cmedit get <FDN>,SystemFunctions=1,SwInventory=1, SwVersion=1
```

21.7.3 Troubleshooting Steps for AXE Nodes

Steps

1. Check the value of the InventoryFunction syncStatus and InventorySupervision active attribute using the ENM CLI.

```
cmedit get NetworkElement=<networkElement>,SHMFunction=1,InventoryFunction=1
```

```
cmedit get NetworkElement=<networkElement>,InventorySupervision=1
```

The InventoryFunction syncStatus must be SYNCHRONIZED and the InventorySupervision active must be true.

2. If the InventoryFunction syncStatus attribute is UNSYNCHRONIZED and InventorySupervision active attribute is false, set InventorySupervision active to true.

```
cmedit set NetworkElement=<networkElement>,InventorySupervision=1 active=tru →
e
```

If the InventoryFunction syncStatus changes to SYNCHRONIZED, the AXE hardware information is displayed.

Note: It can take a few minutes for the `InventoryFunction syncStatus` to change to `SYNCHRONIZED`.

3. If the `InventoryFunction syncStatus` remains `UNSYNCHRONIZED` and no software information is displayed, do a manual sync.

```
cmedit action NetworkElement=<networkElement>,SHMFunction=1,InventoryFunctio →
n=1 synchronize
```

If the `InventoryFunction syncStatus` changes to `SYNCHRONIZED`, the AXE software inventory information is displayed.

Note: It can take a few minutes for the `InventoryFunction syncStatus` to change to `SYNCHRONIZED`.

4. If no software information is displayed after performing the manual sync, contact Ericsson support.

Before contacting Ericsson support, check if the `InventoryFunction syncStatus` is `SYNCHRONIZED`. If yes, run the following command and collect the output.

```
cmedit get <FDN>,Inventory=1,SoftwareInventory=1
```

5. Run the following command to view the first-level data in the CLI.

```
cmedit get <nodename> SoftwareVer.*
```

Example

```
cmedit get <nodename> SoftwareVer.*
FDN : MeContext=MSCSBC029AP1,Inventory=1,SoftwareInventory=1,SoftwareVer=1
administrativeData : {}
componentName : MSCSBC029AP1_CP2
release : M60LCNG250L06A
softwareVersionId : 1
timeOfActivation : null
timeOfInstallation : null
```

First-level data is shown in the CLI.

On running the following command, second-level data is shown in the CLI.

```
cmedit get <nodename> SoftwareItm.*
```

Example

```
cmedit get MSCSBC029AP1 SoftwareItm.*
FDN : MeContext=MSCSBC029AP1,Inventory=1,SoftwareInventory=1,SoftwareItm=1
administrativeData : {productNumber=cxp9027891, productDate=Thu Aug 23 18:16:57 IST 201 →
8, productName=ERIC-sec-cert-agent-cxp9027891, productRevision=2.8.0-024.sle12, product →
Type=SwItem, productDescription=ERIC-sec-cert-agent-cxp9027891}
```

```
softwareItemId : 1
type : SwItem
```

If the second-level inventory details are shown in the output, then collect the output and contact Ericsson Support.

6. Due to node having large number of SoftwareInventory MOs (including child MOs), no **SoftwareInventory** is displayed in UI or SoftwareInventory MO is not updated with `lastsuccesssync`. It results in more time for winfiol to respond Inventory json to shm. So, change the following PIB values to 90, as a result, axe inventory sync time out is increased to 15 min from shm.

```
ericsson/pib-scripts/etc/config.py update --name=AXE_INV_MAX_ →
RETRY_COUNT_TO_QUERY_WINFIOL --app_server_address=<mscmapg se →
rvice group id>:8080 --service_identifier=axe-shm-inventory-m →
ediation-handlers --value=90
```

Execute the following command in physical environment to fetch the service group id from ms:

```
cat /etc/hosts | grep mscmapg
```

Execute the following command in vENM environment to fetch the service group id from vnflaf:

```
consul members | grep mscmapg
```

Note: Values to be updated to `AXE_INV_MAX_RETRY_COUNT_TO_QUERY_WINFIOL` differs based on number of MOs on the Node.

21.8 Troubleshoot Upgrade Jobs

In SHM, the Upgrade Job enables you to upgrade the node according to the selected software package. Node software upgrade is used to install new features on the node and correct the faults in the existing software.

The following table lists error scenarios that may occur while executing the Upgrade Job.The table also lists the related failure message displayed in the *Job Logs* page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
Upgrade Job fails on the selected nodes with Job Logs message "Node is not in sync with ENM"	For the Upgrade Job to be successful, the nodes must be synchronized with ENM.
Upgrade Job fails on the selected nodes with Job Logs message "Error detected in the IP address of the FTP server"	The FTP server used for downloading load modules is not accessible. For a Upgrade job to be successful, the connection between ENM and node must be active.

Scenario	Comment
Upgrade Job fails on CPP based nodes with Job Logs message "The maximum number of allowed CVs will be exceeded if the required number of new CVs is created automatically during an upgrade"	If the number of CVs on a node exceeds the specified limit, the upgrade job cannot be created. Check if the number of CVs on the node exceeds the limit, delete the oldest CV, and re-create the upgrade job
Upgrade Job fails on CPP based nodes with Job Logs message "Upgrade Package is not ready for installation"	Upgrade Package is not ready for installation when either install/upgrade is already executing on the node, or the package is waiting for confirmation or the package is only allowed to delete. Check the "`state`" attribute value while retrieving `UpgradePackage` MO
Upgrade Job fails on CPP based nodes with Job Logs message "Precheck for "Confirm" is failed. Reason: "UpgradePackage" MO not found"	For Upgrade Job to be successful, the precheck for `Confirm` activity must be passed and `UpgradePackage` MO must be present.
Upgrade Job fails on CPP based nodes with Job Logs message "Unable to proceed "Install" Activity because of insufficient inputs"	For Upgrade Job to be successful, the Install activity must be passed. Check whether the imported upgrade package is exists in the ENM.
Upgrade Job fails on ECIM based nodes with Job Logs message "Unable to proceed prepare activity because upgrade package is not in a state to be prepared"	For Upgrade Job to be successful, the upgrade package must be in 'PREPARED' state. Retrieve the Upgrade Package MO with status.
Upgrade Job fails on ECIM based nodes with Job Logs message "Couldn't find software package. Unable to proceed action for node <NodeName>"	For Upgrade Job to be successful, the software package must be present to proceed action on the node. Check whether the imported upgrade package is exists in the ENM.
Upgrade Job fails on ECIM based nodes with Job Logs message "Unable to proceed "verify" activity because UpMo state is not Prepare completed"	For Upgrade Job to be successful, the Verify activity must be successful and the UpMo state must be PREPARE_COMPLETED. Execute the Prepare activity again.
Upgrade job fails on the selected nodes with the Job Logs Message "<Activity name> activity has failed" after the configured timeout value.	Activity may have taken a longer time to execute on the node than the configured timeout value in ENM. Check if the activity has been completed on the node.
Scenario - Upgrade Job fails on AXE based nodes with Job Logs message - "Script execution is failed or interrupted for activity : <ActivityName> due to 'Session=<sessionId>, Exception occured while performing upgrade: The file <filename/filepath> cannot be accessed" on page 161	For Upgrade Job to be successful, the software package must be present to proceed action on the node. Check whether the imported upgrade package exists in ENM.

21.8.1 Scenario - Upgrade Job fails on the selected nodes with Job Logs message - "Node is not in sync with ENM"

For Upgrade Job to be successful, the node must be synchronized. To resolve the node synchronization status, execute the following steps for CPP and ECIM based nodes:

Steps

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the ENM CLI :

```
cmedit get NetworkElement=<networkElement>,CmFunction=1
```

```
cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
```

The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and and the `CmNodeHeartbeatSupervision active` attribute must be `true`.

2. If the CmFunction syncStatus is UNSYNCHRONIZED and CmNodeHeartbeatSupervision active is false, change CmNodeHeartbeatSupervision active to true:

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

   Note: It may take few seconds for the CmFunction 'syncStatus' attribute value to change to 'SYNCHRONIZED'. When the node is in 'SYNCHRONIZED', execute the upgrade job.

3. If the CmFunction syncStatus attribute remains UNSYNCHRONIZED, perform a manual sync:

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

4. If the CmFunction 'syncStatus' attribute value is still 'UNSYNCHRONIZED', then contact Ericsson support for further assistance.

21.8.2 Scenario - Upgrade Job fails on the selected nodes with Job Logs message - "Error detected in the IP address of the FTP server"

The FTP server used for downloading load modules is not accessible. For a Upgrade job to be successful, the connection between ENM and node must be active. For CPP & ECIM based nodes, execute the following steps:

Steps

1. Ensure that the SFTP connection is enabled on the node and the PORT is opened.

   Refer to page 296.

2. Create the Upgrade job again once the connection is established between ENM and Node.

21.8.3 Scenario - Upgrade Job fails on CPP based nodes with Job Logs message - "The maximum number of allowed CVs will be exceeded if the required number of new CVs is created automatically during an upgrade"

If the number of CVs on a node exceeds the specified limit, the upgrade job cannot be created. Check if the number of CVs on the node exceeds the limit, delete the oldest CV, and re-create the upgrade job. To troubleshoot the issue, execute the following steps:

The maximum number of backups that can be stored on a CPP node is 50. This value is not configurable.

Steps

1. In the SHM UI, launch the *Backup Administration* page and add the relevant CPP node using **Network** > **Add Topology Data** drop-down.

   The Backups table lists all the backups that exist for this node. The column Location indicates if the backup is stored on the NODE or in ENM.

2. Check the total number of backups stored on the Node (Location is NODE).

3. If the number of backups on the node is equal to 50, delete the oldest 5 backups creating a Delete Backup Job.

4. Once the delete backup job is successful, create the upgrade job on the node again.

21.8.4 Scenario - Upgrade Job fails on CPP based nodes for Install activity with Job Logs message - "Upgrade Package is not ready for installation"

Upgrade Package is not ready for installation when either install/upgrade is already executing on the node, or the package is waiting for confirmation or the package is only allowed to delete. To troubleshoot the issue, execute the following steps:

Steps

1. Retrieve the `UpgradePackage` MO with following command in ENM CLI Application.

   Retrieve the SwManagement FDN and use the FDN to retrieve upgrade package MO with the required package name you want to upgrade.

   ```
   cmedit get NetworkElement=<networkElement> SwManagement
   ```

   ```
   cmedit get <FDN>,UpgradePackage=<Package Name>
   ```

   Check the "`state`" attribute value from the command response. If the "`state`" attribute value is INSTALL_EXECUTING / UPGRADE_EXECUTING, wait until the action gets finished. If the "`state`" attribute value is AWAITING_CONFIRMATION, the upgrade is finished and waiting for the confirmation. If the "`state`" attribute value is ONLY_DELETEABLE, the package is only allowed to delete.

2. If the state attribute in the response is in any one of the above mentioned values, the job execution is not proceeded.

21.8.5 Scenario - Upgrade Job fails on CPP based nodes with Job Logs message - "Precheck for "Confirm" is failed. Reason: "UpgradePackage" MO not found"

The error scenario occurs when an UpgradePackage MO is deleted by other user/ operation when the current upgrade job execution is in progress. To troubleshoot the issue, execute the following steps:

Steps

1. Verify if the `UpgradePackage` MO exists on the node and ENM using the following ENM CLI command.

   Retrieve the SwManagement FDN and use the FDN to retrieve upgrade package MO with the required package name you want to upgrade.

   ```
   cmedit get NetworkElement=<networkElement> SwManagement
   ```

   ```
   cmedit get <FDN>,UpgradePackage=<Package Name>
   ```

2. If no instances are found in the response for above command, create the upgrade package MO by executing the Upgrade Job with the install activity.

21.8.6 Scenario - Upgrade Job fails on CPP based nodes with Job Logs message - "Unable to proceed "Install" Activity because of insufficient inputs"

For Upgrade Job to be successful, the Install activity must be passed. In this case, verify whether the upgrade package is deleted by other user or operation while the job execution. To troubleshoot the issue, execute the following steps:

Steps

1. In the SHM UI, launch the *Software Administration* page. Click **View Software Packages** link in the quick action bar. The Software Packages table displays a list of all the imported software packages.
2. If the required package is not listed, import the software package into ENM.
3. In the *Software Administration* page, click **Import Software Package** to import the required package.
4. Create the upgrade job again on the node with the imported package.

21.8.7 Scenario - Upgrade Job fails on ECIM based nodes with Job Logs message - "Unable to proceed prepare activity because upgrade package is not in a state to be prepared"

The `Prepare` activity fails if the upgrade package state is not in '`INITIALIZED`'. For Upgrade Job to be successful, the upgrade package must be in '`PREPARED`' state. To troubleshoot the issue, execute the following steps:

Steps

1. Retrieve the `UpgradePackage` MO with following command in ENM CLI application. Retrieve the SystemFunctions FDN and use the FDN to retrieve `upgradepackage` MO with the required package name you want to upgrade.

   ```
   cmedit get <networkElement> SystemFunctions
   ```

   ```
   cmedit get <FDN>,SwM=1,UpgradePackage=<Package Name>
   ```

2. If the status is not in '`INITIALIZED`' state, which means some other activity is ongoing on that MO and wait for its completion.
3. If the issue is still not resolved, then contact Ericsson support for further assistance.

21.8.8 Scenario - Upgrade Job fails on ECIM based nodes with Job Logs message - "Couldn't find software package. Unable to proceed action for node <NodeName>"

For Upgrade Job to be successful, the software package must be present to proceed action on the node. In this case, verify whether the upgrade package is deleted by other user or operation while the job execution. To troubleshoot the issue, execute the following steps:

Steps

1. In the SHM UI, launch the *Software Administration* page. Click **View Software Packages** link in the quick action bar. The Software Packages table displays a list of all the imported software packages.
2. If the required package is not listed, import the software package into ENM.
3. In the *Software Administration* page, click **Import Software Package** to import the required package.
4. Create the upgrade job again on the node with the imported package.

21.8.9 Scenario - Upgrade Job fails on ECIM based nodes with Job Logs message - "Unable to proceed "verify" activity because UpMo state is not Prepare completed"

For Upgrade Job to be successful, the UpMo state must be PREPARE_COMPLETED to proceed/start the `Verify` activity. In this case, the UpMo state is not PREPARE_COMPLETED for the verify action to get triggered. To troubleshoot the issue, execute the following steps:

Steps

1. Check the `UpMo` state with the following ENM CLI command application.

   Retrieve the SwManagement FDN and use the FDN to retrieve upgrade package MO with the required package name you want to upgrade.

   ```
   cmedit get NetworkElement=<networkElement> SwManagement
   ```

   ```
   cmedit get <FDN>,UpgradePackage=<Package Name>
   ```

2. The `Prepare` activity needs to be performed again on the node from SHM UI by creating the upgrade job on the same node with same package.

After This Task

If none of the troubleshooting steps resolves the issue, contact Ericsson support for further assistance.

21.8.10 Scenario - Upgrade Job fails on AXE based nodes with Job Logs message - "Script execution is failed or interrupted for activity : <ActivityName> due to 'Session=<sessionId>, Exception occured while performing upgrade: The file <filename/filepath> cannot be accessed"

For Upgrade Job to be successful, the software package must be present to proceed action on the node. In this case, verify whether the upgrade package is deleted by other user or operation while the job execution. To troubleshoot the issue, execute the following steps:

Steps

1. In the SHM UI, launch the *Software Administration* page. Click **View Software Packages** link in the quick action bar. The Software Packages table displays a list of all the imported software packages.
2. If the required package is not listed, import the software package into ENM.
3. In the *Software Administration* page, click **Import Software Package** to import the required package.

4. Create the upgrade job again on the node with the imported package.

21.8.11 Scenario - Upgrade Job fails on Router6000 series nodes with Job Logs message - "Unable to proceed Verify activity". Reason: "UpMo state is not Prepare completed"

The error scenario occurs during the execution of an Upgrade Job on the Router6000 series node using an UpgradePackage with MO in a 'Waiting for Commit' state.

To troubleshoot the issue, execute the following steps in ENM CLI

 Identify the <upgradePackageId> having the corresponding product revision in the UpgradePackage MO from CM CLI

cmedit get <networkElement>
UpgradePackage.administrativeData

 Verify and confirm whether the UpgradePackage MO state on the NetworkElement is WAITING_FOR_COMMIT

 cmedit get
MeContext=<networkElement>,ManagedElement=1,SystemFunctions=
1,SwM=1,UpgradePackage=<upgradePackageId>

 Execute the CANCEL action operation to deactivate the uncommitted UpgradePackage on the node

cmedit action
MeContext=<networkElement>,ManagedElement=1,SystemFunctions=
1,SwM=1,UpgradePackage=<upgradePackageId>
cancel

 Verify and confirm the UpragePackage state to be rolled back to PREPARE_COMPLETED

cmedit get MeContext= <networkElement
>,ManagedElement=1,SystemFunctions=1,SwM=1,UpgradePackage=<
upgradePackageId>

21.9 Troubleshoot Delete Backup Jobs

In SHM, the Delete Backup Job deletes a backup present on the node or in ENM.

The following table lists error scenarios that may occur while executing a Delete Backup Job. The table also lists the related failure message displayed in the Job Logs page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
Delete Backup Job Fails on CPP based Nodes with Job Logs Message: "CV:<currentLoadedConfigurationVersion> cannot be deleted as it is setStartable or it is the current loaded version"	As the selected CV is set as the Startable Configuration Version or currently loaded Configuration Version while creating the backup, it cannot be deleted.
Delete Backup Job Fails on CPP based Nodes with Job Logs Message:"cannot be deleted as it is in RollbackList"	As the selected CV is present in the Rollback List, it can be deleted only if it is deleted from the rollback list.

21.9.1 Scenario - Delete Backup Job Fails on CPP based Nodes with Job Logs Message - "cannot be deleted as it is in RollbackList"

> As the selected CV is present in the Rollback List, it can be deleted only if it is deleted from the rollback list.

1. In the SHM UI, launch the Backup Administration page and add the relevant node using **Network** > **Add Topology Data** drop-down.

   The `Backups` table lists all the backups that exist for this node.

2. Select the backup to be deleted in the `Backups` table and click **Delete** on the action bar.

3. The Delete Backup dialog box is displayed with the option 'Delete from Rollback List'. Select the option and create the Delete Backup job.

After This Task

If none of the troubleshooting steps resolves the issue, contact Ericsson support for further assistance.

21.10 Troubleshoot Delete Upgrade Package Job

In **Software Hardware Manager** (SHM), the **Delete Upgrade Package** job enables you to delete selected upgrade packages on the node.

The following table lists error scenarios that can occur while executing the **Delete Upgrade Package** job. The table also lists the related failure message displayed in the **Job Logs** page. The relevant procedures to troubleshoot and fix these issues are described.

Scenario	Comment
The **Delete Upgrade Package** job fails on the selected nodes. The **Job Logs** message is as follows:	For the **Delete Upgrade Package** job to be successful, select the following CLI options:

Scenario	Comment
`Upgrade package with product number: <productNumber> and product revision: <productRevision> have delete preventing CVs`	— For CPP-based nodes, select `delRollList`. — For ECIM-based nodes, select `delRefBackups`.
The **Delete Upgrade Package** job fails on the selected nodes. The **Job Logs** message is as follows: `Upgrade package with product number: <productNumber> and product revision: <productRevision> have delete preventing UPs.`	For the **Delete Upgrade Package** job to be successful, select the following CLI options: — For CPP-based nodes, select `delRollList`.
The **Delete Upgrade Package** job fails on CPP-based nodes. The **Job Logs** message is as follows: `CV:<currentLoadedConfigurationVersion> cannot be deleted as it is Startable CV or it is the current loaded version.`	If the deletion of referred backups of the upgrade package being deleted is ongoing, the startable CVs and Current Loaded CVs cannot be deleted.
The **Delete Upgrade Package** job fails on the selected nodes. The **Job Logs** message is as follows: `Failed to delete the Upgrade Package with the ProductNumber <productNumber> and Product Revision <productRevision> From Node.`	The deletion of an upgrade package in context can fail for the following reasons: — Unable to delete any of the referred backups. — Unable to delete any of the referred upgrade packages.
The **Delete Upgrade Package** job fails on the selected nodes. The **Job Logs** message is as follows: `selected upgradePackage with product Number: <productNumber> and Revision: <productRevision> is not available on Node.` .	If the upgrade package is not available, the **Delete Upgrade Package** job is skipped.
The **Delete Upgrade Package** job fails on the selected nodes. The **Job Logs** message is as follows: `selected upgradePackage with product Number: <productNumber> and Revision: <productRevision> is active package on node.`	As the selected upgrade package is already active, it cannot be deleted.

21.11 Troubleshoot View Upgrade Packages in the UI and in the CLI

In SHM, the **View Upgrade Packages** functionality enables you to view upgrade packages on the node.

Prerequisites

The user performing the troubleshooting has one of the following roles:

— `shm_operator`

— `shm_administrator`

The relevant nodes have the following settings:

— CM synchronization is in a `SYNCHRONIZED` state.

— Inventory Supervision is turned on.

Steps

The following table lists error scenarios that can occur while attempting to view upgrade packages on the node. The relevant procedures to troubleshoot and fix these issues are described in the Resolution column.

Scenario	Resolution

The `shm listups` command fails in the CLI. The following error message is displayed:
`Error 13904 : Could not find any NetworkElements in the system for Node type "MSC-BC-IS"`
This error can occur when the user specifies an invalid collection or saved search in the command syntax. For example, when the user executes the following commands:
`shm listups -ne MSC-BC-IS`
	Ensure that Network Elements of the specified NE type have been added to ENM.

The `shm listups` command fails in the CLI. The following error message is displayed:
`Error 13905 : Invalid Network Element type 'sgsn-mme'`
This error message can display in the following circumstances:
— The NE type specified is in the wrong case.
— The NE type specified is not an exact match of the NE type of the deployed model.
The following command uses the correct case to specify the NE type and does not return an error:
`shm listups -ne SGSN-MME`
The following command uses the incorrect case to specify the NE type and returns an error:
`shm listups -ne sgsn-mme`
	Specify the NE type value correctly in the `shm listups` command.

The `shm listups` command response displays an unsupported node table. The following error message is displayed:
`Node Model information is not available.`
This same issue can occur in the **Software Hardware Manager** UI in the **Software Administration** page. Upgrade Packages are not displayed under Upgrade Packages on nodes tab with the following error:
`Selected node(s) are not supported for this view. For more details, please read the 'i' icon tooltip text on the Network Panel.`
These error messages are displayed in the following circumstances:
— The node is in an `UNSYNCHRONIZED` state.
— The node does not support the "Delete Upgrade Packages" feature.
	For CPP-based nodes, perform CM synchronization and inventory synchronization before attempting to view the upgrade packages.
	For ECIM-based nodes, perform CM synchronization before attempting to view the upgrade packages.
	Check that the "Delete Upgrade Packages" feature is supported for the node in context.

21.12 ECIM Node Time Stamps Do Not Use the ENM Time Zone in SHM Administration Pages

> Time stamps for ECIM nodes must use the ENM time zone.

The administration pages of Software Hardware Management display inventory information about the supported nodes in your network. The node time stamps displayed (represented using the **Node Date** field) are converted from the node time zone to the ENM time zone.

The following are not node time stamps and are therefore not converted to the ENM time zone:

— **Production Date** in **Hardware and Software Inventory**

— **Start Date** and **Expiry Date** in **License Inventory**.

Steps

1. Check if offset information (XXX in below format) exists for the time stamp on the node. The time stamp is in the following format.

   ```
   yyyy-MM-dd'T'HH:mm:ss<XXX>
   ```

   Example: `2013-05-01T06:00:00+02:00` (`+02:00` is the offset of Node Time)

2. If offset information does not exist, check if time zone information exists for the Network Element.

   ```
   cmedit get <NodeName> NetworkElement.timeZone
   ```

3. If time zone information does not exist and an offset value does not exist for the Network Element, the timezone has to be set in NetworkElement to display the Node time stamp in ENM time zone correctly.

4. If the time zone is set correctly for the Network Element, but the node time stamps are not set to the ENM time zone, verify the following in the ENM CLI:

   — The value of the `CmFunction syncStatus` attribute is `SYNCHRONIZED`.

   ```
   cmedit get NetworkElement=<networkElement>,CmFunction=1
   ```

   — The active attribute `CmNodeHeartbeatSupervision` is true.

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

5. If the `CmFunction syncStatus` is `SYNCHRONIZED` and the active attribute of `CmNodeHeartbeatSupervision` is true, contact Ericsson Support for further assistance.

21.13 Troubleshoot Automated Software Upgrade Flow

> Automated Software Upgrade (ASU) flow includes a sequence of activities that are executed in an end-to-end NE software upgrade rollout process.

ASU includes the execution of the following jobs:

- Backup Job
- Delete Backup Housekeeping Job.
- Install License Key Files Job.
- Upgrade Job
- Node Health Check
- Enable FM Supervision.
- Script Execution

Execution and report of flow can be monitored in the **Report** tab of the **Flow Instance Details** page.

Note: For detailed information on failure of jobs, user can view the contextual link provided in the **Flow Automation** UI for respective nodes.

The following table lists error scenarios that can occur in ASU flow. The relevant procedures to troubleshoot and fix the issues are described in the later subsections.

Table 6

Scenario	Action
Failure because of authentication	To perform ASU, the user must possess the predefined roles.
Access denied. *<User>* does not exist or unauthorized to perform operations on all or some of the nodes.	For user to perform actions on the node, user must have access to the target node. Contact system administrator for the access.
When a Backup Job for ASU fails	See troubleshooting guidelines for Backup Job in Troubleshoot Backup Jobs on page 134.
When a Backup Housekeeping Job for ASU fails	See troubleshooting guidelines for Backup Housekeeping Job in Troubleshoot Delete Backup Jobs on page 162.
When Upgrade Job of ASU fails	See troubleshooting guidelines for Upgrade Jobs inTroubleshoot Upgrade Jobs on page 155.
When Delete Upgrade Package Job of ASU fails	See troubleshooting guidelines for Upgrade Jobs in Troubleshoot Delete Upgrade Package Job.
When Node Health Check fails for a node in ASU.	See section *Node Health Check Troubleshooting* in ENM Troubleshooting Guide.
Scenario - "Validation Error" During File Input Execution on page 168	Check that valid inputs are provided in file input.
When License Key File installation is skipped in ASU.	See Troubleshoot Install License Key Jobs on page 142.
Scenario - Automated Software Upgrade Flow is Skipped at Upgrade Job on page 168	Selected software package is active on the node.
Scenario - Flow Instance has Stopped on page 169	From the SHM, NHC, cancel the remaining jobs in `WAIT_FOR_USER-INPUT` state, and toggle FM_supervision.
Scenario - Automated Software Upgrade is Triggered on the Same Node Immediately on page 170	ASU flow fails at NHC report as sufficient space is not present in node.

Scenario	Action
Scenario - Automated Software Upgrade Failed When Node Is Migrated from OSS-RC to ENM on page 170	ASU flow fails at NHC report as sufficient space is not present in node.
Scenario - Script Execution Failed Because of a Time-Out on page 171	The script stopped executing because it was not completed within the time-out specified by user. Trigger ASU again, this time ensuring that a higher value is assigned to the **Timeout for execution in seconds** setting.
Scenario - Upgrade Package Validation Fails With "Upgrade cannot be performed as the package is not available on the node" on page 171	Check whether the selected software package exists on the node.
Scenario - Upgrade Package Validation Fails with "Software Package is already available on the node and in ACTIVATION_COMPLETED or any other state" on page 172	The selected software package is not in proper state to proceed with the activation phase.
Scenario - Upgrade Package Validation Fails with "Software Package is already installed and running on the node" on page 172	The selected software package for activation is already installed on the node.

21.13.1 Scenario - "Validation Error" During File Input Execution

— Check the reason for the failure that shows in the pop-up and provide a valid JSON file.

21.13.2 Scenario - Automated Software Upgrade License Key File Job Has Failed at SHM

Cause

Make sure that the latest License Key Files are present in ENM.

Solution

1. In the **SHM** UI, launch the **License Administration** page. Click **Import License Key** from the quick action bar.
2. Browse for the License Key Files. Click **Import**.
3. Once the License Key Files are imported, restart the ASU flow.

21.13.3 Scenario - Automated Software Upgrade Flow is Skipped at Upgrade Job

Cause

If the node is already on the same software level as selected in ASU inputs, upgrade job and the flow is skipped.

Solution

1. Re-trigger the ASU flow.
2. Select a different software package to upgrade.

21.13.4 Scenario - Flow Instance has Stopped

Cause

When the ASU flow Instance is stopped, further activities from the instance are not executed and remain in `WAIT_FOR_USER_INPUT` state.

Solution

1. Do the following steps when `Stop` functionality is used.

Scenario	Steps
SHM Jobs	a. Launch the **Software Hardware Manager** page from **Launcher**. b. In **SHM job** page, filter job name using **FA*your flow Instance name**. For example, **FA*Test**. c. Cancel the SHM jobs that are in `WAIT_FOR_USER_INPUT` state.
NHC Reports	a. Launch the **Node Health Check** page from **Launcher**. b. In **NHC reports** page, filter report name using **FA*your flow Instance name**. For example, **FA*Test**. c. Cancel the activities that are in `WAIT_FOR_USER_INPUT` state in **Node Health Check** page.
FM_SUPERVISION	a. Launch **alarm-management** page from **Launcher**. b. Check the `Supervision` state for a particular node. c. Toggle `FM_SUPERVISION` to `previous` state.

21.13.5 Scenario - Automated Software Upgrade is Triggered on the Same Node Immediately

Cause

A gap of one hour must be observed from **Time of Activation** of software package to do an ASU upgrade on the same node.

Solution

The following steps re-trigger and executes the ASU flow successfully.

1. Launch **Software Hardware Manager** page from **Launcher**.
2. Go to **Software Administration**.
3. Add a node from **Add Topology Data**.
4. In **Software Information**, select the **Table Settings** widget and add **Time of Activation** column.
5. Check the **Time of Activation** for the package that has **Active** column as **YES**.
6. If the time difference between **Time of Activation** and current time is more than one hour, re-trigger the ASU flow from Flow Automation to upgrade the node.

21.13.6 Scenario - Automated Software Upgrade Failed When Node Is Migrated from OSS-RC to ENM

Cause

Node is migrated from OSS-RC to ENM and ASU flow triggered on node has failed.

Solution

The following steps re-trigger and execute the ASU flow successfully.

1. Check the `rbsConfigLevel` in `ManagedElement::NodeSupport::Auto Provisioning MO`.
2. If the `rbsConfigLevel` is in `SITE_CONFIG_COMPLETE(1)`, set it to `READY_FOR_SERVICE(4)`.

Wait for few seconds so that the system created backup on the migrated upgrade package is deleted.

3. Re-trigger the ASU flow from Flow Automation to upgrade the node.

21.13.7 Scenario - Script Execution Failed Because of a Time-Out

> This error occurs when the script execution fails because of a time-out. The proposed solution is only possible if you select the default option **Prompt for Confirmation** when you execute the script.

Solution

1. Open the **Reports** tab, then, under **Node Status**, in the **Contextual Link** column, click **View**.

   In the **User Tasks** screen that opens, you can view **Task: Review Script Failure**.

2. Select **Retry Script execution** in **Task: Review Script Failure**.

3. Change the value of **Timeout for execution in seconds**, and click **Submit**.

21.13.8 Scenario - Upgrade Package Validation Fails With "Upgrade cannot be performed as the package is not available on the node"

This error occurs if the upgrade package selected for the activation is not available on the node. To proceed with the activation flow on that node perform the following steps:

1. From the **Launcher**, launch the **Software Hardware Manager** page.

2. Click **Create Job** and select **Upgrade Job**.

3. Select the nodes and software packages.

4. For ECIM nodes, select the **prepare** and **verify** activities. For CPP nodes, select the **install** and **verify** activities.

5. Once the job is completed:

   — Select **Retry Upgrade Package Validation** to perform the validation or

— Select **Do not Exclude node from Upgrade** to proceed with the activation in **Task: Review Upgrade Package Failure**.

21.13.9 Scenario - Upgrade Package Validation Fails with "Software Package is already available on the node and in ACTIVATION_COMPLETED or any other state"

This error occurs if the upgrade package is not in any of the following states:

— `PREPARE_COMPLETED`

— `INSTALL_COMPLETED`

— `COMMIT_COMPLETED`

— `UPGRADE_COMPLETED`

1. To proceed with activation on this node:

   — For ECIM nodes, revert the upgrade package to the `PREPARE_COMPLETED` state. For CPP nodes, revert the upgrade package to the `INSTALL_COMPLETED` state. OR

   — Select **Exclude node from Upgrade** in **Task: Review Upgrade Package Failure** to stop the flow on the node.

21.13.10 Scenario - Upgrade Package Validation Fails with "Software Package is already installed and running on the node"

This error occurs if the upgrade package selected for activation is already active on the node. No action is required in this case from the operator perspective.

21.14 Onboard Jobs

> Onboard Job enables you to onboard the software package to NFVO (Network Function Virtualization orchestration).

The following table lists error scenarios that may occur while executing the Onboard Job.The table also lists the related failure message displayed in the *Job Logs* page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Table 7

Scenario	Comment
Onboard Job fails on the selected software packages with Job Logs message "Connection refused (Connection refused)".	For the Onboard Job to be successful, there should be proper connectivity between ENM and NFVO.
Delete software package Job fails for virtual software packages with Job Logs message "Package is already in use".	For the Delete software Package job to be successful,the package should not be used by VNF.

21.14.1 Onboard Job fails on the Selected Software Packages with Job Logs Message "Connection refused (Connection refused)"

For Upgrade Job to be successful, there should be proper connectivity between ENM and NFVO. To resolve this connectivity issue, execute the following steps:

Steps

1. Log into mscmce and check connectivity of NFVO by pinging the IP.

   Command: `ping NFVOip`

2. Data loss will be seen while pinging the ip which indicates the IP is corrupted.

3. Configure the correct IP again by using the below command in CLI.

```
 cmedit set NetworkFunctionVirtualizationOrchestrator=<NFVO NAME>,HttpConnectivityInformation=1 ip →
Address="<NFVO_IP>"
```

4. After configuring, try to ping the ip from mscmce which should be reachable.

5. As NFVO connection is fine onboard job should be successful.

21.14.2 Delete Software Package Job fails for Virtual Software Packages with Job Logs Message - "Package" is already in use"

For Delete Job to be successful, the package should not be in use by any VNF. To resolve this issue, execute the following instruction for vRAN based nodes:

Ensure that package is not used by any VNF managed by NFVO.

21.15 Troubleshoot the License Request Job

> In SHM, the License Request job enables the instant generation of License Key Files (LKF) and the installation of these files on selected nodes.

The following table lists error scenarios that can occur while executing the License Request Job. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Cause	Short Description
Cause 1: License Request Job Fails on the Selected Nodes with Job Logs Message "Node Is Not in Sync with ENM" on page 175	For the License Request Job to be successful, the nodes must be synchronized with ENM.
Cause 2: Request Activity Fails with State "LKF_REQUEST_FAILED" on page 175	License Key Files were not generated. The job got failed. Error information from ELIS is displayed.
Cause 3: Request Activity Fails with State "License Keys Files Parsing Failed" on page 176	ENM is not able to parse the License Key Files received from ELIS.
Cause 4: License Request Job Fails on the Selected Nodes with the Job Logs Message "<Activity name> Activity Has Failed" After the Configured Time-Out Expires on page 176	Activity is taking a longer time than expected. Check job logs for additional information.
Cause 5: License Request Job Fails Because ENM Is Not Configured with ELIS and CAS-C on page 176	Check if ENM is configured with ELIS and CAS-C.
Cause 6: Operator Cannot Trigger Capacity LKF Refresh or LKF Refresh Jobs Because Instantaneous Licensing Mode Attribute Is Not Set Correctly on page 177	Check if the `mode` attribute on IL MO is configured as `FULL_ACTIVATION`.
Cause 7: License Request Job Fails with Error Code RBS_CONFIGURATION_INCORRECT on page 178	Check if the Node Instantaneous Licensing MO `euft`, `swltid` parameters are configured correctly.
License Request job fails with error code `ENM_CONFIGURATION_INCOMPLETE`.	Follow the steps mentioned in the *Configurable Parameters for Instantaneous Licensing* and *Activation of Instantaneous Licensing in ENM* sections of the [8] ENM Configuration System Administrator Guide.

Cause 1: License Request Job Fails on the Selected Nodes with Job Logs Message "Node Is Not in Sync with ENM"

For License Request Job to be successful, the node must be synchronized. To resolve the node synchronization status, execute the following steps.

Solution

1. Check the value of the `CmFunction syncStatus` attribute and the value of the `CmNodeHeartbeatSupervision active` attribute using the ENM CLI:

   ```
   cmedit get NetworkElement=<networkElement>,CmFunction=1
   ```

   ```
   cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
   ```

   The `CmFunction syncStatus` attribute must be `SYNCHRONIZED` and the `CmNodeHeartbeatSupervision active` attribute must be `true`.

2. If the `CmFunction syncStatus` is `UNSYNCHRONIZED` and `CmNodeHeartbeatSupervision active` is false, change `CmNodeHeartbeatSupervision active` to `true`:

   ```
   cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
   ve=true
   ```

   Note: It can take a few seconds for the `CmFunction syncStatus` attribute value to change to `SYNCHRONIZED`. When the node is in `SYNCHRONIZED`, execute the job.

3. If the `CmFunction syncStatus` attribute remains `UNSYNCHRONIZED`, perform a manual sync:

   ```
   cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
   ```

4. If the `CmFunction syncStatus` attribute value is still `UNSYNCHRONIZED`, then contact Ericsson support for further assistance.

Cause 2: Request Activity Fails with State "LKF_REQUEST_FAILED"

Error information from ELIS is displayed. The request activity fails with the following state `LKF_REQUEST_FAILED`.

Solution

Contact Ericsson support.

Cause 3: Request Activity Fails with State "License Keys Files Parsing Failed"

This parsing of License Key Files in `shmserv` fails because XML files from ELIS are not in the expected format. The request activity fails with the following state:

```
License Keys Files Parsing Failed
```

Solution

Contact Ericsson support.

Cause 4: License Request Job Fails on the Selected Nodes with the Job Logs Message "<Activity name> Activity Has Failed" After the Configured Time-Out Expires

The job logs message is as follows:

```
<Activity Name> activity has failed.
```

An activity has exceeded an ENM time-out value when executing on the node or fetching files from the Electronic License Information System (ELIS).

Solution

Contact Ericsson support.

Cause 5: License Request Job Fails Because ENM Is Not Configured with ELIS and CAS-C

Solution

Check if ENM is configured with the Electronic License Information System (ELIS) and with the Network Element Software Store (CAS-C). For information about configuring CAS-C, see [8] ENM Configuration System Administrator Guide. If you have difficulties, contact Ericsson support.

Cause 6: Operator Cannot Trigger Capacity LKF Refresh or LKF Refresh Jobs Because Instantaneous Licensing Mode Attribute Is Not Set Correctly

For the License Request Job to be successful, configure the node with Instantaneous Licensing MO attribute `mode` set to`FULL_ACTIVATION`. To set the `mode` attribute, execute the following steps.

Solution

1. Check if the `mode` attribute on the Instantaneous Licensing MO is configured as `FULL_ACTIVATION`:

   ```
   cmedit get SubNetwork=<NetworkElementName>,MeContext=<NetworkElementName>,Ma →
   nagedElement=<NetworkElementName>,NodeSupport=1,LicenseSupport=1,Instantaneo →
   usLicensing=1 --attribute mode
   ```

   Example

   ```
   cmedit get SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio00001,Ma →
   nagedElement=NR01gNodeBRadio00001,NodeSupport=1,LicenseSupport=1,Instantaneo →
   usLicensing=1 --attribute mode
   ```

   Result:

   ```
   FDN : SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio00001,Managed →
   Element=NR01gNodeBRadio00001,NodeSupport=1,LicenseSupport=1,InstantaneousLic →
   ensing=1
   mode : FULL_ACTIVATION
   ```

2. If required, set the `mode` attribute as `FULL_ACTIVATION`:

   ```
   cmedit set SubNetwork=<NetworkElementName>,MeContext=<NetworkElementName>,Ma →
   nagedElement=<NetworkElementName>,NodeSupport=1,LicenseSupport=1,Instantaneo →
   usLicensing=1 mode=FULL_ACTIVATION
   ```

   Example

   ```
   cmedit set SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio00001,Ma →
   nagedElement=NR01gNodeBRadio00001,NodeSupport=1,LicenseSupport=1,Instantaneo →
   usLicensing=1 mode=FULL_ACTIVATION
   ```

   Result:

   ```
   SUCCESS FDN : SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio00001 →
   ,ManagedElement=NR01gNodeBRadio00001,NodeSupport=1,LicenseSupport=1,Instanta →
   neousLicensing=1
   ```

Cause 7: License Request Job Fails with Error Code RBS_CONFIGURATION_INCORRECT

For the License Request Job to be successful, ensure that the `euft` and `swltid` parameters of the Node Instantaneous Licensing MO are configured correctly.To check these parameters, execute the following steps.

Solution

1. Check the `euft` value on the Instantaneous Licensing MO

```
cmedit get SubNetwork=<NetworkElementName>,MeContext=<NetworkElementName>,Ma →
nagedElement=<NetworkElementName>,NodeSupport=1,LicenseSupport=1,Instantaneo →
usLicensing=1 --attribute euft
```

   Example

```
cmedit get SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNod →
eBRadio00001,ManagedElement=NR01gNodeBRadio00001,NodeSupport= →
1,LicenseSupport=1,InstantaneousLicensing=1 --attribute euft
```

   Result:

```
FDN :
SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio0000 →
1,ManagedElement=NR01gNodeBRadio00001,NodeSupport=1,LicenseSu →
pport=1,InstantaneousLicensing=1
euft : 949525
```

2. Check the `swltId` value on the Instantaneous Licensing MO

```
cmedit get SubNetwork=<NetworkElementName>,MeContext=<NetworkElementName>,Ma →
nagedElement=<NetworkElementName>,NodeSupport=1,LicenseSupport=1,Instantaneo →
usLicensing=1 --attribute swltId
```

   Example

```
cmedit get SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNod →
eBRadio00001,ManagedElement=NR01gNodeBRadio00001,NodeSupport= →
1,LicenseSupport=1,InstantaneousLicensing=1 --attribute swltI →
d
```

   Result:

```
FDN :
SubNetwork=NR01gNodeBRadio00001,MeContext=NR01gNodeBRadio0000 →
1,ManagedElement=NR01gNodeBRadio00001,NodeSupport=1,LicenseSu →
pport=1,InstantaneousLicensing=1
swltId : 19DZ725311F4595D22D12666
```

21.16 Troubleshoot Generic SHM Job Issues

21.16.1 Scenario: Fluctuation in the Main Job Progress Percentage

In SHM, the main jobs page displays all the SHM jobs available in the system, along with the details, such as progress percentage and status. User can encounter fluctuation in the progress percentage for the ongoing job.

Solution

No action is required from the user. Progress percentage automatically gets corrected with a small delay. The fluctuation is caused because of a known limitation in the Neo4J leader, follower delay.

Note: For more information, see the [33] Neo4j Documentation.

21.16.2 Scenario: Delay in Main Jobs to Render Newly Created Jobs

In SHM, the main jobs page displays all the SHM jobs that are available in the system. There can be a delay in main jobs page whenever there is load on the Neo4J DB.

Solution

No action is required from the user. The main jobs page automatically gets displayed with a small delay. The fluctuation is caused because of a known limitation in the Neo4J leader, follower nodes.

Note: For more information, see the [33] Neo4j Documentation.

21.16.3 Scenario: Delay in Job Details Page

User can encounter delay or fluctuation in the job status, result, and progress percentage in the job details page whenever there is a load on the Neo4J DB.

Solution

No action is required from the user. The job details are displayed correctly with some delay. The delay is caused because of a known limitation in Neo4J leader, follower nodes.

Note: For more information, see the [33] Neo4j Documentation.

22 VNF-LCM Troubleshooting

> This section provides the troubleshooting steps recommended to diagnose, and fix common problems in the ENM VNF Life Cycle Manager (VNF-LCM) on a cloud deployment.

22.1 VNF-LCM Launch Displays Unable to Retrieve Data Error

When VNF-LCM is launched from ENM launcher, the '`Unable to Retrieve Data`' error can happen if VNFLAF-services VM external IP is not accessible from ENM, or if JBoss server is stopped.

Follow the next sections to troubleshoot these issues.

Note: VNF Life Cycle Manager is a value pack commercial offering. The link is available in the ENM launcher . However, if VNF-LCM is not installed in the cloud, the message `Unable to Retrieve Data Error` is shown when the user clicks on it.

22.1.1 Verify VNF-LCM Accessibility from ENM

If VNF-LCM is unable to retrieve data, check if the installed VNF-LCM VMs are configured and accessible from ENM physical server

Prerequisites

— Access to ENM Management Server (MS-1)

— root login credentials for all VMs and Services of ENM physical

— External IP address of VNFLAF-services VM deployed in cloud.

Steps

1. Log on to ENM MS as the **`litp-admin`** user and switch to **`root`** user.

```
# ssh litp-admin@<MS-1>
# su -
```

2. Get the `Hostname` of first httpd VM.

```
# grep 'httpd' /etc/hosts|grep -i svc|awk '{print $1" "$2}'
```

Example output:

```
[root@ieatclvmlms907 ~]# grep 'httpd' /etc/hosts|grep -i svc|awk '{print $1" "$2}'
10.247.246.42 svc-2-httpd
10.247.246.41 svc-1-httpd
```

3. Use the `Hostname` previously retrieved to log on to the first svc instance of httpd

```
# ssh -i /root/.ssh/vm_private_key cloud-user@svc-1-httpd
```

4. Verify svc-vnflcm host entry is present in `/etc/hosts` file of httpd VM that you are logged.

```
# grep -i svc-vnflcm /etc/hosts
```

Example Output:

```
[cloud-user@svc-1-httpd ~]$ grep -i svc-vnflcm /etc/hosts
131.160.159.165 svc-vnflcm
```

5. Verify vnflaf-services VM of cloud is accessible.

```
# ping -c 1 <IP of vnflaf-services> && echo "vnflaf-services is accesible"
```

Example output:

```
[cloud-user@svc-1-httpd ~]$ ping -c 1 131.160.159.165 && echo "vnflaf-services is accesible"
PING 131.160.159.165 (131.160.159.165) 56(84) bytes of data.
64 bytes from 131.160.159.165: icmp_seq=1 ttl=61 time=0.224 ms

--- 131.160.159.165 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.224/0.224/0.224/0.000 ms
vnflaf-services is accesible
```

Note: If above command returns output "`vnflaf-services is accessible`" and still giving "`Unable to retrieve data`" error, refer to section Verify that VNF-LCM Services are Running to continue verification.

If above command doesn't return output "`vnflaf-services is accesible`", refer to page 296 and check if the network is configured properly in VNFLAF-services VM. If network is configured correctly, and still it is not reaching ENM physical network, then contact Local Ericsson Support to fix the network issue.

22.1.2 Verify VNF-LCM Services are Running

If VNF-LCM VMs are accessible from ENM physical server but they're still unable to retrieve data, verify that JBoss service is running and the relevant files are deployed in it.

Prerequisites

— Execute Verify VNF-LCM Accessibility from ENM task.

— External IP address of VNFLAF-services VM deployed in cloud.

— `cloud-user` and `root` login credentials of VNF-LCM VMs deployed in cloud.

Steps

1. Log on to `VNFLAF-services` VM using external IP.

```
# ssh cloud-user@<External IP of VNFLAF-services VM>
```

2. Switch to `root` user

```
[cloud-user@vnflaf-services ~]$ sudo su -
```

3. Run the following command to verify JBoss is running

```
[root@vnflaf-services ~]# service jboss status
jboss-as is running
```

4. Run the following command to start the JBoss if not running

```
# service jboss start
```

5. Once Jboss is online, verify all files are deployed in `/ericsson/3pp/jboss/standalone/deployments/` folder.

```
Example of deployed file: workflow-file-name.deployed
```

Note: A successfully deployed file should have a copy with same file name appended as deployed.

Example output:

```
camunda-engine-rest-7.7.0-ee.war
camunda-engine-rest-7.7.0-ee.war.deployed
```

After This Task

If the issue is not resolved by this troubleshooting contact Local Ericsson Support.

22.2 Unable to Launch VNF-LCM GUI Using External IP of Services VM

Unable to load the **Workflows** page when the user tries to launch VNF-LCM GUI from the browser using external IP of Services VM.

Prerequisites

— Access to Cloud environment where VNF-LCM is deployed.

— User credentials for logging on to the cloud.

— VNF-LCM is deployed in either in CEE, RHSOP, or OpenStack. For vCD, steps to open VM console differs.

Steps

1. Log on to the **Cloud dashboard**.
2. Go to the **Instances** page and identify the VNF-LCM services VM.
3. Open the VNF-LCM services VM console.
4. Run the following command to check if the IP address is configured in VM interfaces (eth0/eth1).

   ```
   # ip a s
   ```

   Note: IP address updated in VNF-LCM SED and IP address configured in VM interfaces must be same.

5. Check if all the IP details are correct in the `/etc/sysconfig/network-scripts/ifcfg-ethX` file.

   Example

   ```
   # cat /etc/sysconfig/network-scripts/ifcfg-eth1
   DEVICE='eth1'
   TYPE='Ethernet'
   BOOTPROTO='static'
   USERCTRL='yes'
   PEERDNS='yes'
   ONBOOT='yes'
   MTU=1500
   IPV6INIT='no'
   PERSISTENT_DHCLIENT='1'
   PREFIX=25
   IPADDR=131.160.159.45
   GATEWAY=131.160.159.1
   ```

6. Do one of the following:

   — If IP details are correct in the `/etc/sysconfig/network-scripts/ifcfg-ethX` file, it is a Network issue. Contact Cloud Administrator.

— If IP details are not correct, check the `/ericsson/vnflcm/data/host.properties` file to verify that the following Network details are correct.

```
external_subnet_cidr=131.160.159.0/25
external_ip_address=131.160.159.45
external_gateway=131.160.159.1
external_mtu=1500
internal_subnet_cidr=172.16.100.0/24
internal_ip_address=172.16.100.55
internal_gateway=172.16.100.1
internal_mtu=1500
```

— If Network details are not correct, then redeploy VNF-LCM stack using the correct Network details in SED.

22.3 Troubleshoot JBoss Failures

This section provides steps for a solution to JBoss failures.

22.3.1 Check VNF-LCM dB VM is Accessible

Prerequisites

— Access to VNF-LCM services VM over external IP.

— User credentials for logging on to Services VM.

Steps

1. Log on to VNF-LCM services as cloud user using the `key_pair.pem`.

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
```

Note: — Use the default password **passw0rd** and when prompted, provide the new password.

— If login reports `Connection refused error`, wait for a few minutes.

2. Switch to root user.

```
# sudo su -
```

3. Ping VNF-LCM dB VM.

```
# ping vnflaf-db
```

Example

```
# ping -c 1 vnflaf-db
PING vnflaf-db (172.16.100.53) 56(84) bytes of data.
64 bytes from vnflaf-db (172.16.100.53): icmp_seq=1 ttl=64 time=0.080 ms

--- vnflaf-db ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.080/0.080/0.080/0.000 ms
```

4. Do one of the following:
   - If ping fails, go to section Configure VNF-LCM dB VM on page 185.
   - If ping is successful, go to section Check PostgreSQL Configuration on page 186.

22.3.2 Configure VNF-LCM dB VM

Prerequisites

- Access to Cloud environment where VNF-LCM is deployed.
- User credentials for logging on to the cloud.

Steps

1. Log on to the cloud dashboard.
2. Go to **Instances** page and identify the VNF-LCM dB VM.
3. Open the VNF-LCM dB VM console.
4. Run the following command and check if IP address is configured in VM interfaces.

```
# ip a s
```

5. Check the `/etc/sysconfig/network-scripts/ifcfg-ethX` file to see if the IP details are correct.

   Example

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE='eth1'
TYPE='Ethernet'
BOOTPROTO='static'
USERCTRL='yes'
PEERDNS='yes'
ONBOOT='yes'
MTU=1500
IPV6INIT='no'
PERSISTENT_DHCLIENT='1'
PREFIX=25
IPADDR=131.160.159.45
GATEWAY=131.160.159.1
```

6. Do one of the following:

   — f IP details are correct in the `/etc/sysconfig/network-scripts/ifcfg-ethX` file, it is a Network issue. Contact Cloud Administrator.

   — If IP details are not correct, check the `/ericsson/vnflcm/data/host.properties` file to verify that the following Network details are correct.

   ```
   external_subnet_cidr=131.160.159.0/25
   external_ip_address=131.160.159.45
   external_gateway=131.160.159.1
   external_mtu=1500
   internal_subnet_cidr=172.16.100.0/24
   internal_ip_address=172.16.100.55
   internal_gateway=172.16.100.1
   internal_mtu=1500
   ```

   — If Network details are not correct, then redeploy VNF-LCM stack using the correct Network details in SED.

22.3.3 Check PostgreSQL Configuration

Prerequisites

— Access to VNF-LCM services VM over external IP.

— User credentials for logging on to VNF-LCM services VM.

— User credentials for logging on to VNF-LCM dB VM.

— Access to VNF-LCM SED file.

Steps

1. Log on to VNF-LCM services as cloud user using the `key_pair.pem`.

   ```
   # ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
   ```

   Note: — Use the default password **`passw0rd`** and when prompted, provide the new password.

   — If login reports `Connection refused` error, wait for a few minutes.

2. Switch to root user.

   ```
   # sudo su -
   ```

3. Log on to VNF-LCM dB VM from VNF-LCM Services VM using **internal_ipv4_for_db_vm** or internal **internal_ipv6_for_db_vm** as cloud user.

```
# ssh cloud-user@<internal_IP_for_db_vm>
```

Note: Use the default password **passw0rd** and when prompted, provide a new password.

4. Switch to root user.

```
# sudo su -
```

5. Find the internal Network subnet CIDR from `host.properties` file.

```
# grep -i internal_subnet_cidr /ericsson/vnflcm/data/host.properties
internal_subnet_cidr=172.16.100.0/24
internal_subnet_cidr6=
```

Use value of `internal_subnet_cidr` if `ip_version` is 4 or dual.

Use value of `internal_subnet_cidr6` if `ip_version` is 6.

6. Check if the `internal subnet cidr` mentioned in the previous step is added in the PostgreSQL `pg_hba.conf` file.

```
# grep -i 172.16.100.0/24 /vnflcm-ext/current/db/data/pg_hba.conf
host    all             all             172.16.100.0/24         md5
```

7. If internal subnet CIDR is present in `pg_hba.conf` file, then go to section Check Network MTU Configuration on page 188.

8. If internal subnet CIDR not present in `pg_hba.conf` file, then add the following line manually under `# IPv4 local connections:` section in the `pg_hba.conf` file.

```
host    all             all             172.16.100.0/24         md5
```

9. Save the file and restart the PostgreSQL service.

```
# systemctl restart rh-postgresql94-postgresql
```

10. Return to VNF-LCM services VM.

11. Restart the JBoss service.

```
# systemctl restart jboss
```

12. If JBoss fails to start, go to section Check Network MTU Configuration on page 188.

22.3.4 Check Network MTU Configuration

Prerequisites

— Access to `keystonerc` file for deployment.

— Access to a client machine to run OpenStack operation. For small Integrated ENM solution, Virtual Management Server must be used as the client machine.

— Access to VNF-LCM services VM over external IP.

— User credentials for logging on to VNF-LCM services VM.

Steps

1. Log on to VNF-LCM services as cloud user using the `key_pair.pem`.

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
```

Note: — Use the default password **`passw0rd`** and when prompted, provide a new password.

— If login reports `Connection refused error`, wait for a few minutes.

2. Switch to root user.

```
# sudo su -
```

3. Run the following command to get the MTU values configured for interfaces.

```
# cat /ericsson/vnflcm/data/host.properties | grep -i mtu
```

4. Run the following command to find the MTU of Network, which is used for configuring interfaces.

```
# openstack network show <network name> | grep -i mtu
```

5. Compare the MTU values obtained in *step 3* and *step 4*.

Note: MTU configured in the internal and external interface must be compared with MTU of internal and external Networks respectively.

6. If the MTUs are not correct, then redeploy VNF-LCM stack using the correct MTU values in SED.

7. Log on to VNF-LCM dB VM from VNF-LCM Services VM using **`internal_ipv4_for_db_vm`** or **`internal_ipv6_for_db_vm`** as cloud user.

```
# ssh cloud-user@<internal_IP_for_db_vm>
```

Note: Use the default password **passw0rd** and when prompted, provide a new password.

8. Switch to the root user.

```
# sudo su -
```

9. Restart PostgreSQL service.

```
# systemctl restart rh-postgresql94-postgresql
```

10. Return to Services VM.

11. Restart JBoss service.

```
# systemctl restart jboss
```

12. If JBoss service fails to start, then collect the following logs from VMs and contact VNF-LCM with a support ticket.

```
/var/log/cloud-init-output.log
/ericsson/3pp/jboss/standalone/log/server.log
```

22.4 Unable to Reach External VIP of VNF-LCM Services VM

Prerequisites

— Access to VNF-LCM services VM over external IP.

— User credentials for logging on to services VM.

— VNF-LCM SED file

Steps

1. Log on to VNF-LCM services as cloud user using the `key_pair.pem`.

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
```

Note:
— Use the default password **passw0rd** and when prompted, provide a new password.

— If login reports `Connection refused error`, wait for a few minutes.

2. Switch to root user.

```
# sudo su -
```

3. Collect the following logs from VM.

```
/var/log/vnflcm/.health_check.log
/var/log/vnflcm/.svc_check.log
```

4. Log on to VNF-LCM dB VM from VNF-LCM Services VM using **internal_ipv4_for_db_vm** or **internal_ipv6_for_db_vm** as cloud user.

```
# ssh cloud-user@<internal_IP_for_db_vm>
```

5. Switch to root user.

```
# sudo su -
```

6. Collect the following logs from VM.

```
/var/log/vnflcm/.health_check.log
/var/log/vnflcm/.db_check.log
```

22.5 VNF-LCM Workflow Execution Error Sceneries

> During the execution of a workflow which invokes ECM (Ericsson Cloud Manager) or CEE (Cloud Execution Environment) Rest call, there's a change of failure in case of a valid ECM or CEE certificate isn't installed in JBoss, or vnflaf-services VM is unable to resolve the Host name of ECM or CEE.

In the first scenario, the JBoss server log file displays the error message: "`IOException:: sun.security.validator.ValidatorException:PKIX path building failed:sun.security.provider.certpath.SunCertPathBuilderException`", and in the case of missing Host name, the log displays "`IOException:: No route to host`" or "`UnknownHostException`" error messages.

Follow the next sections to troubleshoot these issues.

22.5.1 Resolve Host Name to Connect to Cloud Manager

Resolve ECM or CEE Host name when workflow Rest call fails.

Prerequisites

— `Root` and `cloud-user` access to the vnflaf-services VM.

— A command console is opened.

— User knows the Host name and IP Address of CEE or ECM.

Steps

1. Log on to vnflaf-services VM as `cloud-user`.
2. Switch to `root` user.
3. Check if ECM or CEE host details are added to the hosts file.

   ```
   [root@vnflaf-services ~]# less /etc/hosts | grep "<host-name or IP>"
   ```

   Example

   ```
   [root@vnflaf-services ~]# less /etc/hosts | grep "ecmapp"
   131.160.150.45 ecmapp.domain.com
   ```

4. If entry is not found, open `/etc/hosts` file and add it in below format.

   ```
   <IP address of ECM or CEE> <host-name>
   ```

Results

User does not see the error message in the server log, and gets proper response for the workflow.

22.5.2 Install a Valid ECM or CEE Certificate on VNF-LCM Workflow Failure

Install a valid ECM or CEE certificate when workflow Rest call fails.

Prerequisites

— `Root` and `cloud-user` access to the vnflaf-services VM

— A command console is opened

— User knows the Hostname/IP Address of CEE or ECM

Steps

1. Log on to vnflaf-services VM as `cloud-user`.
2. Switch to `root` user.
3. Download the SSL certificate from CEE using the following command:

```
[root@vnflaf-services ~]# openssl s_client -showcerts -connect <CLOUD MANAGE →
R HOSTNAME>:<PORT NUMBER OF KEYSTONE SERVICE> < /dev/null | openssl x509 -ou →
tform DER > /tmp/sslcert.cer
```

Note: If the above downloaded certificate does not contain complete chain of the certificates (from host certificate up to the root CA certificate), it is required to get the missing link in the certificate chain from the respective certificate authority. For private CA certificates, the corresponding cloud admin needs to be contacted. If it's a public CA certificate, then it can be downloaded from the corresponding website.

4. Download the SSL certificate from ECM using the following command:

```
[root@vnflaf-services ~]# openssl s_client -showcerts -connect <ECM HOSTNAME →
 or ECM IP ADDRESS>:443 < /dev/null | openssl x509 -outform DER > /tmp/ecm_c →
ert.cer
```

5. Remove the CA certificate alias from the system if it already exists.

```
[root@vnflaf-services ~]# <JDKPATH>/bin/keytool -delete -keystore  <JDKPATH> →
/jre/lib/security/cacerts -alias <CA CERTIFICATE ALIAS>
```

6. Install the certificate into the system.

```
[root@vnflaf-services ~]# <JDKPATH>/bin/keytool -import -alias <CA CERTIFICA →
TE ALIAS> -file /tmp/ecm_cert.cer -keystore <JDKPATH>/jre/lib/security/cacer →
ts -storepass changeit
```

Note: `<JDKPATH>` is the JDK installed directory path (For example, /usr/java/jdk1.7.0_95).

Results

User does not see the error message in the server log, and gets proper response for the workflow.

Example 5

```
[root@vnflaf-services ~]# openssl s_client -showcerts   -connect  <hostname>:500 →
0  < /dev/null | openssl x509 -outform PEM > /tmp/ssl_cert.cer
depth=2
 C = US, O = "VeriSign, Inc.", OU = VeriSign Trust Network, OU = "(c)
2006 VeriSign, Inc. - For authorized use only", CN = VeriSign Class 3
Public Primary Certification Authority - G5
verify return:1
depth=1 C = US, O = Symantec Corporation, OU = Symantec Trust Network, CN = Syma →
ntec Class 3 Secure Server CA - G4
verify return:1
depth=0 C = SE, ST = Stockholm, L = Stockholm, O = Ericsson, OU = IT, CN = <host →
name>
verify return:1
DONE
```

22.6 Restart Services to Treat Internal Server Error

When VNF Life Cycle Manager application is launched from ENM launcher, the 'Internal Server Error' is displayed if any service in the VMs are stopped. Restart the services to treat this error.

Prerequisites

— VNF-LCM Workflows page reports "internal server Error".

— `Root` and `cloud-user` access to the vnflaf-services and vnflaf-db VMs.

Steps

1. Log on to vnflaf-db VM as `cloud-user` .
2. Switch to `root` user.
3. Restart posgresql94-postgresql service

```
[root@vnflaf-services ~]$ service postgresql94-postgresql restart
```

4. Log on to vnflaf-services VM as `cloud-user`.
5. Switch to `root` user.
6. VM and restart JBOSS service as root user

```
[root@vnflaf-services ~]$ service jboss restart
```

Note: If the issue is not resolved by this troubleshooting contact Local Ericsson Support.

Results

VNF-LCM services are restarted successfully and VNFLCM Workflows page loads without "internal server Error".

22.7 Create VNF Lifecycle Manager Power Up and Power Down Sequence

Use the following sequences to power up and power down.

Power Up

1. Power Up `vnflaf-db VM`.

2. Power Up `vnflaf-services VM`.

Power Down

1. Power Down `vnflaf-services VM`.
2. Power Down `vnflaf-db VM`.

22.8 Recover Faulty VNF-LCM VMs for HA Deployments

> This section describes the procedure to recover faulty `vnflaf-services` VMs for HA deployments.

Prerequisites

— VNF-LCM UI is not accessible over external virtual IP.

— JBoss failed in both `vnflaf-services-0` and `vnflaf-services-1`.

— `vnflaf-services-0` and `vnflaf-services-1` are not accessible because of network failure or compute host evacuation.

Steps

1. Log on to the client machine and set the environment with the `keystonerc` file.
2. Open the OpenStack Client, and go to directory `/VNFLCM/artifacts`.
3. Update VNF-LCM stack.

```
# openstack stack update --wait --existing <deployment_id>_VNFLCM
```

4. Identify the `vnflaf-services` VM resources that are part of VNF-LCM.

```
# openstack stack resource list <deployment_id>_VNFLCM -n3 | egrep -iw "nova::server" | →
 grep -i vnflaf-services
```

The **<deployment_id>_VNFLCM** in the command is the VNF-LCM stack name.

Example

```
# openstack stack resource list ieatenmc4b10_VNFLCM -n3 | egrep -iw "nova::server" | grep -i vnflaf-services
| vnflaf-services | f6100709-951f-4940-8d5b-6818d866c66c | OS::Nova::Server | CREATE_COMPLETE | 2019-03-02T11:17: →
40 | ieatenmc4b10_VNFLCM-vnflaf-services-32us4cnjur6p-1-vndoywsexz7e |
| vnflaf-services | fec9cb73-0908-4093-8d0b-8a8721428306 | OS::Nova::Server | CREATE_COMPLETE | 2019-03-02T11:17: →
41 | ieatenmc4b10_VNFLCM-vnflaf-services-32us4cnjur6p-0-5qj6pp6tn6f2 |
```

5. Mark the resources obtained in *step 4* to unhealthy.

```
# openstack stack resource mark unhealthy <stack-name> vnflaf-services
```

Example

```
# openstack stack resource mark unhealthy ieatenmc4b10_VNFLCM-vnflaf-services-32us4cnjur6p-0-5qj6pp6tn6f2 vnflaf-services
```

6. Update the VNF-LCM stack.

Example

```
# openstack stack update --wait --existing <deployment_id>_VNFLCM
```

7. Follow the post install procedure to set passwords provided in the *VNF-LCM Installation Instructions* and verify restored workflows in `vnflaf-services` VM.

22.9 Recover vnflaf-db VMs from Compute Host Failures for HA Deployments

> This section, which is only applicable to HA deployments of VNF-LCM, first describes how to identify if one or more faulty `vnflaf-db` VMs have had compute host failures. It then describes how to recover the affected `vnflaf-db` VMs.

Verify that the following symptoms exists:

— Launching the VNF-LCM UI over external VIP prompts `Internal Server Error`.

— `vnflaf-db MASTER` is not functional because of compute host failure and `vnflaf-db STANDBY` failed to become `MASTER`. Run the following commands to verify.

```
[root@vnflaf-services-0 ~]# ssh cloud-user@<internal_ipv4_vip_for_db or internal_ipv6_vip_for_db>

ssh: ssh: connect to host vnflaf-db port 22: No route to Host
```

```
[root@vnflaf-services-0 ~]# ssh cloud-user@<internal_ipv4_for_db_vm or internal_ipv6_for_db_vm>
```

Note: Try with both IPs provided for variable `internal_ipv4_for_db_vm` in SED.

```
[root@vnflaf-db-1 ~]# service rh-postgresql94-postgresql status
```

Example

```
[root@dep001-vnflaf-services-0 ~]# ssh cloud-user@10.10.0.157
ssh: connect to host 10.10.0.157 port 22: No route to Host
[root@dep001-vnflaf-services-0 ~]# ssh cloud-user@10.10.0.153
ssh: connect to host 10.10.0.157 port 22: No route to Host
[root@dep001-vnflaf-services-0 ~]# ssh cloud-user@10.10.0.154
[root@dep001-vnflaf-db-1 ~]# service rh-postgresql94-postgresql status
[root@ieatenmc4b10-vnflaf-db-1 ~]# service rh-postgresql94-postgresql status
Redirecting to /bin/systemctl status  rh-postgresql94-postgresql.service
rh-postgresql94-postgresql.service - PostgreSQL database server
 Loaded: loaded (/usr/lib/systemd/system/rh-postgresql94-postgresql.service; enabled; v →
endor preset: disabled)
 Active: failed (dead) since Mon 2019-07-09 06:05:14 IST
```

— Boss failed in both `vnflaf-services-0` and `vnflaf-services-1` because dB is in a failed state. Run the following command to verify.

```
[root@dep001-vnflaf-services ~]# service jboss status
ssh: connect to host 10.10.0.157 port 22: No route to Host
JBOSS: INFO (): jboss-as status check code : 7
JBOSS: ERROR (): jboss-as is not running
```

The following prerequisites are required before running the steps.

— The VNF-LCM deployment is HA.

— The VNF-LCM SED JSON file is available.

— User able to log on to the vnflaf-services VMs using SSH.

1. Log on to the client machine and set the environment with the `keystonerc`.
2. Identify the faulty `vnflaf-db` VM resource part of VNF-LCM stack.

```
# openstack server list | egrep -i <deployment_id> | egrep -i "error" | grep - →
i vnflaf-db
```

The `<deployment_id>` is the value filled for variable `deployment_id` in the SED.

Example

```
# openstack server list | egrep -iw "ieatenmc4b10" | egrep -i "error" | grep →
 -i vnflaf-db
| f6100709-951f-4940-8d5b-6818d866c66c | ieatenmc4b10-vnflafdb-0 | ERROR | v →
nflcm-internal-net=172.16.100.22 | ERICrhelpostgresimage_CXP9032491-4.11.7.q →
cow2 |
```

3. Identify the corresponding faulty `vnflaf-db` VM resource in the VNF-LCM stack.

```
# openstack stack resource list <deployment_id>_VNFLCM -n3 | egrep -iw "nova:: →
server" | grep -i <ID of faulty db VM>
```

The variables in the command are as follows:

— `<deployment_id>_VNFLCM` is the VNF-LCM stack name.

— `<ID of faulty db VM>` is the ID of the faulty database VM returned in the previous step.

Example

```
# openstack stack resource list ieatenmc4b10_VNFLCM -n3 | egrep -iw "nova::s →
erver" | grep -i f6100709-951f-4940-8d5b-6818d866c66c
| vnflaf-db | f6100709-951f-4940-8d5b-6818d866c66c | OS::Nova::Server | CREA →
TE_COMPLETE | 2019-03-02T11:17:40 | ieatenmc4b10_VNFLCM-vnflaf-db-32us4cnjur →
6p-0-vndoywsexz7e |
```

4. Mark the resources obtained in above step to unhealthy.

```
# openstack stack resource mark unhealthy <stack-name> vnflaf-db
```

`<stack-name>` is the stack name returned in command output of the previous step.

Example

```
# openstack stack resource mark unhealthy ieatenmc4b10_VNFLCM-vnflaf-db-32us →
4cnjur6p-0-vndoywsexz7e vnflaf-db
```

5. Update the VNF-LCM stack.

```
# openstack stack update --wait --existing <deployment_id>_VNFLCM
```

Note: — Wait for 10-15 minutes to proceed with rest of the procedure.

— Make sure that stack update is successful. If it fails with the message `"No host available"`, repeat all the steps.

6. Check if the faulty database VM is recreated and available in ACTIVE state.

```
# openstack server list | egrep -i <Faulty db VM Instance Name>
```

`<Faulty db VM Instance Name>` is the instance name (second field) of the faulty database VM returned in *step 3*.

Example

```
# openstack server list | grep-i ieatenmc4b10-vnflafdb-0
   | f6108708-951d-4948-8d5c-6818d866d66d | ieatenmc4b10-vnflafdb-0| ACTIVE  →
| internal-net=172.16.100.22 | ERICrhelpostgresimage_CXP9032491-4.11.7.qcow2 →
 |
```

Note: If the recreated VM is not in an ACTIVE state, run this procedure again.

7. Log on to vnflaf-services-0 VM as cloud-user and switch to root user.

```
# ssh -i <key-pair>.pem cloud-user@<vnflaf-services-0 IP>
[cloud-user@vnflaf-services-0 ~]# sudo su -
```

<Internal VIP for DB VM> is the IP address provided for either of the following variables:

— external_ipv4_for_services

— external_ipv6_for_services in the SED.

8. Log on to vnflcm-db MASTER VM from VNF-LCM Services VM as cloud-user and switch to root user.

Note: For the first login, use the default password passw0rd and enter a new password when prompted.

```
[root@vnflaf-services-0 ~]# ssh cloud-user@<Internal VIP for DB VM>
[cloud-user@vnflaf-db-0 ~]# sudo su -
```

<Internal VIP for DB VM> is the IP address provided for either of the following variables:

— external_ipv4_for_services

— external_ipv6_for_services in the SED.

9. Verify whether PostgreSQL is running.

```
root@db-0-vnflcm# service rh-postgresql94-postgresql status
```

10. Log out from the db VM.

11. Restart the JBoss service on the vnflaf-service-0 VM.

```
root@vnflaf-services-0# service jboss restart
```

12. Verify that the JBoss service is running on the vnflaf-services-0 VM.

```
root@vnflaf-services-0# service jboss status
```

13. Log on to the vnflaf-services-1 VM as cloud-user and switch to root user.

```
# ssh -i <key-pair>.pem cloud-user@<vnflaf-services-1 IP>
[cloud-user@vnflaf-services-1 ~]# sudo su -
```

<vnflaf-services-1 IP> is the second IP address provided for either of the following variables:

— external_ipv4_for_services

— external_ipv6_for_services in SED

14. Restart the JBoss service on vnflaf-service-1 VM.

```
root@vnflaf-services-1# service jboss restart
```

15. Verify that JBoss is running on vnflaf-service-1 VM.

```
root@vnflaf-services-1# service jboss status
```

16. Verify that the VNF-LCM UI is accessible over external VIP, using the value filled for either of the following variables:

— external_ipv4_for_services

— external_ipv6_for_services in SED

22.10 Recover vnflaf-db VMs When Volumes Are Left in "Detaching" Status After the Compute Host Fails

This section describes how to recover one or more faulty vnflaf-db VMs when the following symptoms exist:

— Compute host failure has occurred.

— Volume status is not changing from "detaching" to "available" after the compute host failure.

Note: This section is only applicable to High Availability (HA) deployments of VNF-LCM.

Do not bring the faulty compute host online while performing the steps in this section.

Prerequisites

— The VNF-LCM deployment is HA.

— Either vnflaf-db-0 or vnflaf-db-1 VM is down because of compute host failure or shutdown.

— The volume attached to the faulty VM is left in a Detaching state.

— The progress for the VNF-LCM High Availability workflow associated with the faulty VM is stuck at 20%. The workflow is stuck at the `Detaching Cinder Volume` step.

— The VNF-LCM SED json file and HOT Files are available.

— It is still possible to log in to the `vnflaf-services` MASTER VM using VIP.

— The VNF-LCM deployment is still operational using the URL for the UI.

Note: `vnflaf-db-1` VM is the faulty database VM in all examples described.

Steps

1. Log on to the `vnflcm-services MASTER` VM using the `key_pair.pem` as `cloud-user` and switch to `root`.

   ```
   # ssh -i <key_pair>.pem cloud-user@<external_vip_for_services>

   [root@dep001-vnflaf-services ~]# sudo su -
   ```

   `<external_vip_for_services_vm>` is the value updated in SED for either `external_ipv4_vip_for_services` or `external_ipv6_vip_for_services`.

2. Disable the auto recovery process of VNF-LCM.

   ```
   [root@dep001-vnflaf-services ~]# vnflcm autorecovery disable
   ```

3. Remove the faulty database VM staging file.

   ```
   [root@dep001-vnflaf-services ~]# rm -rf /vnflcm-ext/.db-<0 or 1>-*
   ```

   `<0 or 1>` is the faulty database VM number.

4. Launch the VNF-LCM UI using the following URL.

   `http://<external_ipv4_vip_for_services>/index.html#workflows/workflow/ha-auto-recovery.--.VNF-LCM%20High%20Availability%20Workflow`

5. Cancel the instance of the running VNF-LCM High Availability workflow for the faulty database VM.

6. Log on to the client machine and set the environment with the `keystonerc` file.

7. Identify which volume in the faulty database VM is left in state `Detaching`.

   ```
   # openstack volume list | grep -i <deployment_id>_vnflcm | grep -i Detaching
   ```

Example:

```
# openstack volume list | grep -i dep001_vnflcm | grep -i Detaching | 39f280 →
7d-c179-453c-8cb8-486e1ce3fb04 | dep001_vnflcm_volume_1 | Detaching | 120 |  →
Attached to dep001-vnflaf-db-1 on | | | | | /dev/vdb |
```

8. Reset the attached volume status for the faulty database VM so that it becomes available.

```
# cinder reset-state --attach-status detached <Faulty_VM_Volume_ID>
```

<Faulty_VM_Volume_ID> is the volume ID obtained in the previous step.

Example:

```
# cinder reset-state --attach-status detached  39f2807d-c179-453c-8cb8-486e1 →
ce3fb04
```

9. Check the volume status.

The volume status must be in Available state.

```
# openstack volume list| grep -i <Faulty_VM_Volume_ID>
```

Example:

```
# openstack volume list | grep -i 39f2807d-c179-453c-8cb8-486e1ce3fb04 | 39f →
2807d-c179-453c-8cb8-486e1ce3fb04 | dep001_vnflcm_volume_1 | Available | 120 →
 | |
```

10. Obtain the following information about the faulty vnflaf-db VM: id, associated port, and stack name.

```
# openstack stack resource list \
<deployment_id>_VNFLCM -n3 |grep -i \
vnflaf-db | grep -i "\-<Faulty_VM_Number>-" | \
egrep -i "nova::server|port"
```

<Faulty_VM_Number> is the number of the faulty database VM; 0 or 1.

Example if faulty VM is vnflaf-db-1:

```
# openstack stack resource list ieatenmc6b01_VNFLCM -n3 |grep -i vnflaf-db | →
 grep -i "\-1-" | egrep -i "nova::server|port" | vnflaf-db | 5b7e915a-ca9f-4 →
aee-aa42-9de3108af2ea | OS::Nova::Server | CREATE_COMPLETE | 2019-07-29T13:4 →
8:12Z | dep001_VNFLCM-vnflaf-db-epjyc6ggxhc3-1-s3kwvrmbf7q5 | | vnflaf_db_in →
ternal_port | 284bc35a-3414-4c8d-b72f-bd71128ed7c8 | OS::Neutron::Port| CREA →
TE_COMPLETE | 2019-07-29T12:46:12Z | dep001_VNFLCM-vnflaf-db-epjyc6ggxhc3-1- →
s3kwvrmbf7q5 |
```

Note the following:

— Resource id of Nova::server

— Resource id of `OS::Neutron::Port`

— Stack name (shown in the last column of the output)

11. Delete the Faulty VM.

```
# openstack server delete <Faulty_VM_id>
```

`<Faulty_VM_id>` is the resource id obtained in the previous step.

Example:

```
# openstack server delete 5b7e915a-ca9f-4aee-aa42-9de3108af2ea
```

12. Delete the port associated with the faulty VM.

```
# openstack port delete <Port_id_of_Faulty_VM>
```

`<Port_id_of_Faulty_VM>` is the resource id of OS::Neutron::Port obtained in step-10.

Example:

```
# openstack port delete 284bc35a-3414-4c8d-b72f-bd71128ed7c8
```

13. Check the VNF-LCM stack.

```
# openstack stack check <deployment_id>_VNFLCM
```

14. Delete the stack of the faulty database VM.

```
# openstack stack delete --wait <Faulty_VM_stack_name>
```

`<Faulty_VM_stack_name>` is the port resource id obtained in step-10, last column value indicates the stack name.

Example:

```
# openstack stack delete \
--wait dep001_VNFLCM-vnflaf-db-epjyc6ggxhc3-1-s3kwvrmbf7q5
```

15. Identify the stack resource of the faulty database VM.

```
# openstack stack resource list \
<deployment_id>_VNFLCM -n3 |grep -i \
vnflaf-db |grep -i yaml | grep \
-w <Faulty_VM_Number>
```

`<Faulty_VM_Number>` is the number of the faulty database VM; 0 or 1.

Example if faulty VM is vnflaf-db-1:

```
# openstack stack resource list dep001_VNFLCM -n3 |grep -i vnflaf-db |grep -
i yaml | grep -w 1 | 1 | 37f51f1c-7f0c-4aee-936a-48702666f95f | file:///VNF-
LCM/Upgrade/artifacts/HOT/Resources/Hotfiles/vnflcm-heat-template-static-cin
der-db.yaml | UPDATE_COMPLETE | 2019-07-29T13:49:44Z | dep001_VNFLCM-vnflaf-
db-epjyc6ggxhc3 |
```

16. Mark the stack resource for the Faulty database VM as unhealthy.

```
# openstack stack resource mark unhealthy <Faulty_VM_stack> <Faulty_VM_Numbe
r>
```

— `<Faulty_VM_stack>` is the stack name obtained above step.

— `<Faulty_VM_Number>` is the number of the faulty database VM; `0` or 1.

Example if Faulty_VM_Number is 1:

```
# openstack stack resource mark unhealthy dep001_VNFLCM-vnflaf-db-epjyc6ggxh
c3 1
```

17. Open the OpenStack Client and change directory to `<path to filesystem>/VNF-LCM/Upgrade/artifacts/HOT/Resources/Hotfiles`.

    This is the path where the media artifacts of the running VNF-LCM are extracted.

18. Update VNF-LCM stack using `sed.json` and `yaml` files.

    These files are the same as what is used for VNF-LCM deployment or upgrade.

```
# openstack stack update --wait \
-e <sed json file> -t \
<YAML file> <deployment_id>_VNFLCM
```

    Use the appropriate `yaml` file for the `ip_version` as described in below table:

ip_version	YAML file
dual	vnflcm-heat-template-static-cinder.yaml
4	vnflcm-heat-template-static-cinder-ipv4.yaml
6	vnflcm-heat-template-static-cinder-ipv6.yaml
dual,6	vnflcm-heat-template-static-cinder-dual-ipv6.yaml

    Note: Wait for about 15–20 minutes before proceeding to the next step.

19. Log on to the `vnflcm-services MASTER` VM using the `key_pair.pem` as `cloud-user` and switch to `root`.

20. Log on to the recovered database VM as cloud-user and switch to root.

    Note: For the first login, use the default password " `passw0rd` " and input a new password if prompted.

21. Restart the `keepalived` service.

    ```
    [root@dep001-vnflaf-db-1 ~]# service keepalived stop
    [root@dep001-vnflaf-db-1 ~]# service keepalived start
    ```

22. Log out of the recovered database VM.

23. Open the `vnflcm-services` MASTER VM and enable the VNF-LCM HA auto-recovery workflow.

    ```
    [root@dep001-vnflaf-services-0 ~]# vnflcm autorecovery enable
    ```

22.11 Recover vnflaf-db VM When "ip_version" in SED is "dual,6"

This section explains how to recover the faulty `vnflaf-db` VM if:

— The `ip_version` in the Site Engineering Document (SED) is `dual,6`.

— It is not possible to launch the UI for the VM.

To fix this error, the user must have the following:

— Access details for the VMs

— `keypair.pem` files for the VMs.

— A Site Engineering Document file.

Steps

1. Log on to the `vnflcm-services` Master VM using the `key_pair.pem` as `cloud-user` and switch to root.

2. Run the following command, replacing `<external_vip_for_services_vm>` with the value updated in the SED for variable `external_ipv6_vip_for_services`.

    ```
    # ssh -i key_pair.pem cloud-user@external_vip_for_services
    ```

3. Shut down the `vnflcm-services` Master VM.

```
# init 0
```

Note: This command logs the user out of the `vnflcm-services` Master VM.

4. Launch the VNF-LCM UI using the IP value filled for variable `external_ipv6_vip_for_services` in the SED for the VNF-LCM VM.
5. Check if the recovery workflow triggered for the following is complete and successful:
   - The faulty `vnflcm-db` VM, which is assigned the number `0` or `1`.
   - The `vnflcm-services` VM, which is assigned the number `0` or `1` and which was shut down in the previous step.

   Note: Wait until completion percentage for each workflow instance is `100%`. When this happens, the VNF-LCM High Availability Workflow has fully recovered the faulty `vnflaf-db` VM.

22.12 Recover a Failed VNF Workflow in a VNF-LCM That Is High Availability

> You can download and run a script that enables you to rerun failed workflows.

This issue occurs if any VNF workflow causes an incident similar to the following:

```
"Cannot deserialize object in variable 'hotParametersMap': SPIN/JACKSON-JSON-010 →
07 Cannot construct java type from string 'groovy.json.internal.LazyMap<java.lan →
g.String,java.lang.Object>'"
```

Prerequisites

- The High Availability VNF-LCM is successfully deployed in Openstack or CEE.
- VNF-LCM SED json is available.
- The required access details and key pair information are available to enable logins to VMs.
- GASK portal access is provided.

Steps

1. Download the following package from GASK.

Table 8 GASK Package Details

Document Number	Revision
2/190 89-CXP 903 4858	A

2. Transfer the downloaded package to the VNF-LCM Services Master VM.

```
# scp -i <key_pair>.pem 2_19089-CXP9034858_X_A_TAR_GZIPV1.tar.gz cloud-user@ →
<external_ipv4/6_vip_for_services_vm> :/vnflcm-ext/vnf-lcm/
```

The variables in the command are as follows:

— `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

— `<external_ipv4/6_vip_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_vip_for_services_vm` or `external_ipv6_vip_for_services_vm`.

3. Establish a secure connection to the VNF-LCM Services Master VM as `cloud-user`.

```
# ssh -i <key_pair>.pem cloud-user@<external_ipv4/6_vip_for_services_vm>
```

The variables in the command are as follows:

— `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

— `<external_ipv4/6_vip_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_vip_for_services_vm` or `external_ipv6_vip_for_services_vm`.

4. Switch to `root` user.

```
[cloud-user@vnflaf-services ~]# sudo su -
```

5. Disable VNF-LCM recovery.

```
[root@vnflaf-services ~]# vnflcm autorecovery disable
```

6. Log out of the VNF-LCM Services Master VM.

7. Establish a secure connection to the VNF-LCM Services-0 VM as `cloud-user` and switch to `root`.

```
# ssh -i <key_pair>.pem cloud-user@<external_ipv4/6_for_services_vm>
```

The variables in the command are as follows:

— `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

— `<external_ipv4/6_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_for_services_vm` or `external_ipv6_for_services_vm`.

8. Switch to `root` user.

```
[cloud-user@vnflaf-services ~]# sudo su -
```

9. Change to the file system directory.

```
[root@vnflaf-services ~]# cd /vnflcm-ext/vnf-lcm/
```

10. Extract the package.

```
[root@vnflaf-services /vnflcm-ext/vnf-lcm/]# tar -xzvf 2_19089-CXP9034858_X_ →
A_TAR_GZIPV1.tar.gz
```

11. Execute the package script.

```
[root@vnflaf-services ~]# python /vnflcm-ext/vnf-lcm/OverwriteJacksonModule. →
py
```

12. Restart the JBoss service.

```
[root@vnflaf-services ~]#  systemctl restart jboss
```

13. Verify that the JBoss service has returned to a running state.

```
[root@vnflaf-services ~]#  systemctl status jboss
```

14. Log out of the VNF-LCM Services-0 VM.

15. Establish a secure connection to the VNF-LCM Services-1 VM as `cloud-user`.

```
# ssh -i <key pair>.pem cloud-user@<external_ipv4/6_for_services_vm>
```

The variables in the command are as follows:

— `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

— `<external_ipv4/6_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED:

`external_ipv4_for_services_vm` or `external_ipv6_for_services_vm`.

16. Switch to `root` user.

```
[cloud-user@vnflaf-services ~]# sudo su -
```

17. Execute the package script.

```
[root@vnflaf-services ~]# python /vnflcm-ext/vnf-lcm/OverwriteJacksonModule.py
```

18. Restart the JBoss service.

```
[root@vnflaf-services ~]#  systemctl restart jboss
```

19. Verify that the JBoss service has returned to a running state.

```
[root@vnflaf-services ~]#  systemctl status jboss
```

20. Log out of VNF-LCM Services-1 VM.

21. Establish a secure connection to the VNF-LCM Services Master VM as `cloud-user`.

```
# ssh cloud-user@<external_ipv4/6_vip_for_services_vm>
```

The variables in the command are as follows:

— `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

— `<external_ipv4/6_vip_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_vip_for_services_vm` or `external_ipv6_vip_for_services_vm`.

22. Switch to `root` user.

```
[cloud-user@vnflaf-services ~]# sudo su -
```

23. Enable VNF-LCM recovery.

```
[root@vnflaf-services ~]# vnflcm autorecovery enable
```

24. Try executing the Virtual Node workflow and verify that it works correctly.

22.13 Recover a Failed VNF Workflow in a VNF-LCM That Is Not High Availability

> You can download and run a script that enables you to rerun failed workflows.

This issue occurs if any VNF workflow causes an incident similar to the following:

```
"Cannot deserialize object in variable 'hotParametersMap': SPIN/JACKSON-JSON-010 →
07 Cannot construct java type from string 'groovy.json.internal.LazyMap<java.lan →
g.String,java.lang.Object>'"
```

Prerequisites

- The VNF-LCM without High Availability is successfully deployed in Openstack or CEE or VCD.
- VNF-LCM SED json is available.
- The required access details and key pair information are available to enable logins to VMs.
- GASK portal access is provided.

Steps

1. Download the following package from GASK.

   Table 9 GASK Package Details

Document Number	Revision
2/190 89-CXP 903 4858	A

2. Transfer the downloaded file to the VNF-LCM Services VM.

   ```
   # scp -i <key_pair>.pem 2_19089-CXP9034858_X_A_TAR_GZIPV1.tar.gz cloud-user@ →
   <<external_ipv4/6_vip_for_services_vm> :/vnflcm-ext/vnf-lcm/
   ```

   The variables in the command are as follows:

   - `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.
   - `<external_ipv4/6_vip_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_vip_for_services_vm` or `external_ipv6_vip_for_services_vm`.

3. Establish a secure connection to the VNF-LCM Services VM as `cloud-user`.

   ```
   # ssh -i <key_pair>.pem cloud-user@<external_ipv4/6_for_services_vm>
   ```

   The variables in the command are as follows:

   — `<key_pair>.pem` is the key pair name filled for variable `key_pair` in the SED.

   — `<external_ipv4/6_for_services_vm>` is the IP before the comma (IP,) for one of the following variables in the SED: `external_ipv4_for_services_vm` or `external_ipv6_for_services_vm`.

4. Switch to `root` user.

   ```
   [cloud-user@vnflaf-services ~]# sudo su -
   ```

5. Change to the file system directory.

   ```
   [root@vnflaf-services ~]# cd /vnflcm-ext/vnf-lcm/
   ```

6. Extract the package.

   ```
   [root@vnflaf-services /vnflcm-ext/vnf-lcm/]# tar -xzvf 2_19089-CXP9034858_X_ →
   A_TAR_GZIPV1.tar.gz
   ```

7. Execute the package script.

   ```
   [root@vnflaf-services ~]# python /vnflcm-ext/vnf-lcm/OverwriteJacksonModule. →
   py
   ```

8. Restart the JBoss service.

   ```
   [root@vnflaf-services ~]#  systemctl restart jboss
   ```

9. Verify that the JBoss service has returned to a running state.

   ```
   [root@vnflaf-services ~]#  systemctl status jboss
   ```

10. Log out of the VNF-LCM Services VM.

11. Try executing the VNF workflow and verify that it works correctly.

22.14 Disable Jboss Logs

> Disable jboss logs that contain password in encoded format, by default it is enabled.

Note: If the VM is recreated (due to rebuild, upgrade, HA event, and so on), this change will be deleted, and must be repeated again.

This is an optional step. It can be enabled or disabled as the need arises.

Prerequisites

— Access to VNF-LCM services VM over external IP.

— User credentials for logging on to Services VM.

— VNF-LCM SED file.

Steps

1. Log on to VNF-LCM services as cloud user using the key_pair.pem

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
```

If deployment type is HA:

Log on to vnflcm-services-0 using the key_pair.pem as cloud-user:

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_ →
vm>
```

Note: For HA deployment same changes should be done in both the services i.e vnflcm-services-0 and vnflcm-services-1.

Use the default password `passw0rd` and when prompted, provide the new password.

If login reports `Connection refused error`, wait for a few minutes.

2. Switch to root user

```
# sudo su -
```

3. Execute following commands to `DISABLE` and `ENABLE` logs:

Note: Execute the following command only once:

```
/ericsson/3pp/jboss/bin/jboss-cli.sh -c --command="/subsystem=loggi →
ng/logger=com.ericsson.oss.services.wfs.jse.impl.WorkflowInstanceSe →
rviceImpl:add(level=INFO)"
```

To `DISABLE` logs, execute the following command:

```
/ericsson/3pp/jboss/bin/jboss-cli.sh -c --command="/subsystem=logging/logger →
=com.ericsson.oss.services.wfs.jse.impl.WorkflowInstanceServiceImpl:write-at →
tribute(name=level,value=OFF)"
```

To `ENABLE` logs, execute the following command:

```
/ericsson/3pp/jboss/bin/jboss-cli.sh -c --command="/subsystem=logging/logger →
=com.ericsson.oss.services.wfs.jse.impl.WorkflowInstanceServiceImpl:add(leve →
l=INFO)"
```

22.15 Unable to Launch a New Workflow Instance after Importing in Geo-Redundant Deployment

> Internal server error occurs while launching a workflow instance after performing an import from backup file in a geo-redundant deployment.

Prerequisites

— Access to VNF-LCM CLI

— User credentials for logging on to the CLI

Solution - For VNF-LCM Non-High Availability

1. Log on to the VNF-LCM services VM as `cloud-user` and switch to `root` user.

```
# ssh -i <key_pair>.pem cloud-user@<external_ip_for_services_vm>
[cloud-user@vnflaf-services ~]# sudo su -
```

2. Log on to the VNF-LCM DB VM from the VNF-LCM Services VM.

```
[root@vnflaf-services ~]# ssh cloud-user@<internal_ip_for_db_vm>
```

3. Execute the following command in the DB VM to delete data from table `act_ru_jobdef`.

```
[root@vnflaf-db~]# sudo -u postgres psql -d wfsdb -c "TRUNCATE TABLE act_ru_ →
jobdef" CASCADE;
```

4. Switch back to the VNF-LCM services VM and restart `JBoss` using the following command:

```
[root@vnflaf-services ~]# service jboss restart
```

Solution - For VNF-LCM High Availability

1. Log on to `vnflcm-services` MASTER VM using the `key_pair.pem` as `cloud-user`.

```
# ssh -i <key_pair>.pem cloud-user@<external_vip_for_services>
```

   Where *<external_vip_for_services_vm>* is the value updated in SED for `external_ipv4_vip_for_services` or `external_ipv6_vip_for_services`.

2. Switch to root user:

```
[cloud-user@vnflaf-services-1 ~]$ sudo su -
```

3. Verify the status of `autorecovery`:

```
[root@vnflaf-services ~]# vnflcm autorecovery status
```

   If `autorecovery` is enabled, disable it by executing the following command:

```
[root@vnflaf-services ~]#  vnflcm autorecovery disable
```

4. Log on to Master DB VM:

```
[root@vnflaf-services ~]# ssh cloud-user@vnflaf-db
```

5. Execute the following command in DB VM to delete data from table `act_ru_jobdef`.

```
[root@vnflaf-db~]# sudo -u postgres psql -d wfsdb -c "TRUNCATE TABLE act_ru_ →
jobdef" CASCADE;
```

   On successful execution exit from DB VM.

6. Log on to Services Standby VM as `cloud-user` and switch to `root`. Use the *<key name>* defined in the SED and value filled for variable *<internal_ipv4_for_services_vm>* or *<internal_ipv6_for_services_vm>* in VNF-LCM SED.

```
# ssh -i <key_pair>.pem cloud-user@<external_vip_for_services>
```

Where *<external_vip_for_services_vm>* is the value updated in SED for `external_ipv4_vip_for_services` or `external_ipv6_vip_for_services`.

7. Switch to root user.

```
[cloud-user@vnflaf-services-0 ~]$ sudo su -
```

8. Restart `JBoss` using the following command:

```
[root@vnflaf-services ~]# service jboss restart
```

9. Switch back to VNF-LCM services Master VM and restart `JBoss` using the following command:

```
[root@vnflaf-services ~]# service jboss restart
```

10. Enable `autorecovery`:

```
[root@vnflaf-services ~]# vnflcm autorecovery enable
```

22.16 SFTP Issues During Upgrade of Indoor Nodes Using Unsecure SBL

Problem

FTP connection failures for indoor nodes that are running unsecure SBL and are configured to use SFTP protocol

Cause

Indoor nodes that are running unsecure SBL and are configured to SFTP protocol for file transfer use SSHv1 as the underlying protocol during SFTP operations. As ENM supports only SSHv2 connections for SFTP therefore SFTP requests on SSHv1 are rejected.

Solution

It is recommended to use unsecure protocols like FTP for nodes running unsecure SBL while managing from ENM.

For nodes running on secure SBL, there is no issue with SFTP as the underlying protocol used in SSHv2.

Note: NeTypes that have unsecured SBL are as follows:

- MINI-LINK-Indoor
- MINI-LINK-CN210
- MINI-LINK-CN510R1
- MINI-LINK-CN510R2
- MINI-LINK-CN810R1
- MINI-LINK-CN810R2

22.17 VNF-LCM SSL Certificate is Showing as Expired

Ignore the VNF-LCM SSL certificate that has expired on 7th March 2020 as it does not impact the VNF-LCM functionality. The VNF-LCM SSL certificate was applicable only for OSSRC deployments. Since OSSRC is out of support, this certificate will be removed in future sprints.

22.18 VNF-LCM Fails to Load New Auto Start Rules

Problem

Auto start rules do not load into the VNF-LCM cache if new rules are added to the `/vnflcm-ext/current/workflows/auto-start-rules` XML file and the watch-service is disabled. This is an intermittent problem and could occur only when the watch-service has stopped working.

Solution

Perform a JBoss restart:

```
#service jboss restart
```

Note: For HA VNFLCM deployments, perform the JBoss restart on the Master `vnflaf-services` VM.

Tip: To access the Master `vnflaf-services`, provide values for the *<external_ipv4_vip_for_services>* or *<external_ipv6_vip_for_services>* variables in the VNFLCM SED.

22.19 Update VNF-LCM Httpd Timeout

Problem

VNF LCM use cases, Instantiate and Scale-Out are getting timed-out with 502 proxy error when the VNF is large in size (Querying all resources from VIM takes more than 2 minutes).

Solution

The httpd timeout should be increased in VNF-LCM from the default value of 120 seconds, to the value which can fulfill the VNF query response time from VIM (preferably 5 minutes).

Perform the following steps to change the httpd timeout value. Ensure that there is no LCM operation ongoing in VNF-LCM during this configuration change.

1. Log on to VNF-LCM VM and switch to root user.
2. Change the Timeout value.

   ```
   sed -i "s/Timeout 120/Timeout 180/" /opt/rh/jbcs-httpd24/root →
   /etc/httpd/conf/httpd.conf
   ```

3. Restart the httpd process.

   ```
   service jbcs-httpd24-httpd restart
   ```

4. Verify the status.

   ```
   service jbcs-httpd24-httpd status
   ```

Tip: Check the timeout value on both EOCM and on ENM Side before configuring the httpd timeout.

23 WinFIOL Troubleshooting

This section provides the troubleshooting steps recommended to diagnose, and fix common problems in the ENM WinFIOL CLI and WinFIOL GUI.

23.1 WinFIOL CLI is Not Available

The WinFIOL CLI link is not available when logged into the ENM UI or from Network Explorer.

Prerequisites

— WinFIOL_Operator role.

— User is assigned with a POSIX Role (Scripting_Operator, Amos_Operator, or Element_Manager_Operator).

Steps

1. Verify that the user has `WinFIOL_Operator` role, and that the user is assigned with a POSIX Role .
2. Log on to ENM as Administrator, and add the appropriate user roles to the user.

Results

WinFIOL CLI link is available.

23.2 WinFIOL GUI Application is Not Available

The WinFIOL GUI link is not available from Network Explorer.

Prerequisites

— WinFIOL_Operator and Element_Manager_Operator roles.

Steps

1. Verify that the user has `WinFIOL_Operator` and `Element_Manager_Operator` user roles.
2. Log on to ENM as Administrator, and add the appropriate user role(s) to the user.

Results

WinFIOL GUI link is available from Network Explorer.

23.3 Unable to Start WinFIOL

If WinFIOL Service Group (SG) has failed or does not come online during Initial Install (II) or Initial Upgrade (IU) within the defined timeout and after maximum number of retries the virtual machine (VM) for the SG is marked as faulted.

Prerequisites

— `root` access to the Management Server (MS-1).

— litp-admin access to Scripting Cluster (SCP).

Steps

1. Log on to ENM MS as a **`litp-admin`** user and switch to **`root`** user.
2. From MS-1 log on to the scp-1 machine as litp-admin and grant `root` access:

```
ssh litp-admin@scp-1
su
```

3. Provide the current status in the Veritas Cluster Service, including faulted service groups, resources, links, or agents by execute command:

```
hastatus -sum
```

Result: Example printout:

```
[root@ieatrcxb5956 ~]# hastatus -sum
 &8211; System State Frozen
A ieatrcxb5956 RUNNING 0
A ieatrcxb5969 RUNNING 0
&8211; GROUP STATE
&8211; Group                                  System       Probed AutoDisable →
d State
B Grp_CS_scp_cluster_amos               ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_amos               ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_elementmanager     ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_elementmanager     ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scripting          ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scripting          ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scriptinglvsrouter ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scriptinglvsrouter ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_winfiol            ieatrcxb5956 Y      N             OFF →
LINE|FAULTED
B Grp_CS_scp_cluster_winfiol            ieatrcxb5969 Y      N             OFF →
```

```
LINE|FAULTED
B Grp_NIC_scp_cluster_bond0_608         ieatrcxb5956 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_bond0_608         ieatrcxb5969 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br0               ieatrcxb5956 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br0               ieatrcxb5969 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br1               ieatrcxb5956 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br1               ieatrcxb5969 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br2               ieatrcxb5956 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br2               ieatrcxb5969 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br3               ieatrcxb5956 Y      N            ONL →
INE
B Grp_NIC_scp_cluster_br3               ieatrcxb5969 Y      N            ONL →
INE
```

The SG that has not started will be marked OFFLINE|FAULTED.

4. Clear the fault systems to be able to restart the SG:

```
hagrp -clear Grp_CS_scp_cluster_winfiol -any
```

This command clears the State of all systems. In this case the both failed WinFIOL SG will be cleared.

   a. To specify only one of the systems use the flag "-sys" followed by the system e.g:

```
hagrp -clear Grp_CS_scp_cluster_winfiol -sys ieatrcxb5956
```

5. Launch the SG again.

```
hagrp -online Grp_CS_scp_cluster_winfiol -sys ieatrcxb5956
```

6. Monitor startup of VM by connecting to virsh console. To list possible VMs run:

```
virsh list --all
```

This command will list all VMs running on this service node and also the VMs that are currently offline. For "Grp_CS_scp_cluster_winfiol" the name is "winfiol".

Result: Example printout:

```
[root@ieatrcxb5956 litp-admin]# virsh list --all
 Id    Name                           State
----------------------------------------------------
 18    scriptinglvsrouter             running
 19    winfiol                        running
 20    scripting                      running
 21    amos                           running
```

```
 22    elementmanager                running
```

7. Connect to the WinFIOL SG:

```
virsh console winfiol
```

Result: Expected printout:

```
[root@ieatrcxb5956 ~]# virsh console winfiol
Connected to domain winfiol
Escape character is ^]
```

The console for winfiol is showing and it is possible to follow the startup of the VM.

8. When the VM started a login prompt will appear.

```
Red Hat Enterprise Linux Server release 6.10 (Santiago)
Kernel 2.6.32-754.8.1.el6.x86_64 on an x86_64
scp-1-winfiol login:
```

9. Exit virsh console by typing <ctrl +]>

10. Verify Grp_CS_scp_cluster_winfiol is online:

```
hastatus -sum
```

Result: Expexted printout:

```
[root@ieatrcxb5956 ~]# hastatus -sum
 &8211; System State Frozen
A ieatrcxb5956 RUNNING 0
A ieatrcxb5969 RUNNING 0
&8211; GROUP STATE
&8211; Group                                    System       Probed AutoDisable →
d State
B Grp_CS_scp_cluster_amos               ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_amos               ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_elementmanager     ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_elementmanager     ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scripting          ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scripting          ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scriptinglvsrouter ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_scriptinglvsrouter ieatrcxb5969 Y      N             ONL →
INE
B Grp_CS_scp_cluster_winfiol            ieatrcxb5956 Y      N             ONL →
INE
B Grp_CS_scp_cluster_winfiol            ieatrcxb5969 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_bond0_608         ieatrcxb5956 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_bond0_608         ieatrcxb5969 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br0               ieatrcxb5956 Y      N             ONL →
INE
```

```
B Grp_NIC_scp_cluster_br0               ieatrcxb5969 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br1               ieatrcxb5956 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br1               ieatrcxb5969 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br2               ieatrcxb5956 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br2               ieatrcxb5969 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br3               ieatrcxb5956 Y      N             ONL →
INE
B Grp_NIC_scp_cluster_br3               ieatrcxb5969 Y      N             ONL →
INE
```

Results

WinFIOL SG is started

24 CM Node Synchronization Troubleshooting - SSR/vBNG/Router8800 Nodes

This section provides troubleshooting steps to diagnose common problems with node synchronization and notification handling of SSR, vBNG, Router8800 nodes.

24.1 Attempt Manual Sync when CM Node Supervision is Deactivated for SSR, vBNG and Router8800

Each node that is managed by ENM has an attribute called `CmNodeHeartbeatSupervision.active`. This attribute can be set to `true` or `false` to notify ENM that the node is targeted for supervision or not. Only supervised nodes can be synchronized with ENM.

Prerequisites

— Basic knowledge of how to use the CM CLI.

Steps

1. If the CM supervision of the node is deactivated and a manual synchronization of the node is triggered in the CM CLI, the synchronization status of the node will be set to UNSYNCHRONIZED.
2. Check if the CM supervision is deactivated for the node, and then activate it.

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    active : false

    1 instance(s)

2)  cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1 active →
=true
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1

    1 instance(s)
```

3. Supervision of the node will automatically be triggered in ENM once the value of `CmNodeHeartbeatSupervision.active` changes state from `false` to `true`. It may take some time for the node to synchronize. Execute the below command until the node state changes to SYNCHRONIZED.

```
1)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : SYNCHRONIZED

    1 instance(s)
```

Results

The node is synchronized with ENM

24.2 SSR, vBNG and Router8800 Nodes polling falling if there is no data on node

The first time ENM attempts to synchronize a node, and ENM will able to sync node with empty data. But it will fail while performing polling on the node.

This guide provides information on steps to identify and troubleshoot this issue.

Prerequisites

— Basic knowledge of how to use the CM CLI.

— Verify server log of mssnmpcm SG

Steps

1. Check if the CM supervision is deactivated for the node, and then activate it.

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    active : false

    1 instance(s)

2)  cmedit set NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1 active →
=true
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1

    1 instance(s)
```

2. Supervision of the node will automatically be triggered in ENM once the value of `CmNodeHeartbeatSupervision.active` changes state from `false` to `true`. It may take some time for the node to synchronize. Execute the below command until the node state changes to `SYNCHRONIZED`.

```
1)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : SYNCHRONIZED

    1 instance(s)
```

3. After some time the sync status will change to `UNSYNCHRONIZED` and in JBOSS server log will get the below error.

```
2017-08-23 10:24:32,510 ERROR [com.ericsson.oss.mediation.cm.snmp.util.MoAtt →
ributeDpsOperation] (default-threads - 5) 'ifTableLastChange' retrieved for  →
'MeContext=NESSvBNG,ManagedElement=NESSvBNG,mib-2=1,ifMIB=1,ifMIBObjects=1'  →
is null.
2017-08-23 10:24:32,511 ERROR [com.ericsson.oss.mediation.cm.snmp.retry.Retr →
yingInterceptor] (default-threads - 5) Failed to execute getMoAttribute meth →
od, not retrying: DpsValueException: 'ifTableLastChange' not retrieved for M →
eContext=NESSvBNG,ManagedElement=NESSvBNG,mib-2=1,ifMIB=1,ifMIBObjects=1
2017-08-23 10:24:32,511 ERROR [com.ericsson.oss.mediation.cm.snmp.polling.Po →
```

```
ller] (default-threads - 5) Could not load DPS value for polling 'com.ericss →
on.oss.mediation.cm.snmp.polling.PollTarget@610265656{checkFdn: mib-2=1,ifMI →
B=1,ifMIBObjects=1, checkAttribute: ifTableLastChange, frequency: 300}' for →
'NetworkElement=NESSvBNG': com.ericsson.oss.mediation.cm.snmp.exception.DpsV →
alueException: 'ifTableLastChange' not retrieved for MeContext=NESSvBNG,Mana →
gedElement=NESSvBNG,mib-2=1,ifMIB=1,ifMIBObjects=1
```

Results

The node is unsynchronized with ENM after sometime.

24.3 SSR, vBNG and Router8800 Nodes Unreachable from ENM

To synchronize with a node, ENM must have a physical connection and the correct network settings between the node and ENM.

The node may be unreachable from ENM for one of the following reasons:

1. ENM specific ports are not available. Refer to page 296.
2. Network connectivity to the node is faulty.
3. The node is stopped, not responding or in an error state. Refer to the *Troubleshooting Guide* in the CPI delivered with the relevant node.
4. The security configuration is invalid or incorrect, and permission is denied during SNMP communication handshake between ENM and the node.

Prerequisites

— Root access to the Management Server (MS).

— Basic knowledge of Linux and JBOSS.

— Basic knowledge of how to use the CM CLI.

Steps

1. If the node that ENM is attempting to synchronize with is unreachable, sync status will be set to `UNSYNCHRONIZED`. To check this run the following commands from the CM CLI

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)

2)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. To confirm that the node is unreachable, the JBOSS logs need to be checked. Log on to the MS and check all MSSNMPCM (Mediation Service SNMP Configuration Management) JBOSS logs as shown below.

   The error message shown below will only be seen on the MSSNMPCM instance that was attempting to synchronize the node.

   The below command when executed will go to all MSSNMPCM instances.

   Refer to the sections *VM Security Tasks* and *Connect to a Virtual Machine* in page 296 to connect to the VMs.

```
2016-10-27 08:17:33,041 ERROR [com.ericsson.oss.mediation.adapter.connector. →
adventnet.AventnetSnmpTable] (EJB default - 191) Error with get bulk for ta →
ble with oid: .1.3.6.1.2.1.2.2 Message: Error: Request Timed Out
2016-10-27 08:17:33,041 ERROR [com.ericsson.oss.mediation.adapter.connector. →
adventnet.AventnetSnmpTable] (EJB default - 191) Error with get bulk for ta →
ble with oid: .1.3.6.1.2.1.2.2 Message: Error: Request Timed Out
2016-10-27 08:17:33,045 ERROR [org.jboss.as.ejb3.invocation] (EJB default -  →
191) JBAS014134: EJB Invocation failed on component SnmpSyncManager for meth →
od public java.util.Map com.ericsson.oss.mediation.snmp.cm.operation.SnmpSyn →
cManager.syncNode(java.lang.String,com.ericsson.oss.mediation.adapter.connec →
tor.api.SnmpConnectionAttributes,java.util.Map) throws javax.resource.Resour →
ceException: javax.ejb.EJBException: com.ericsson.oss.mediation.adapter.conn →
ector.api.exceptions.SnmpTimeoutRuntimeException: Error: Request Timed Out
```

Results

Possible root causes of synchronization failure identified.

24.4 Troubleshoot SSR, vBNG and Router8800 Nodes Synchronization Failure at First Attempt

The first time ENM attempts to synchronize a node, it must calculate the node model identity by reading the Administrative Data (neProductVersion) from the node.

If this operation fails, it looks for the `ossModelIdentity` supplied by the operator and uses it to synchronize the node.

If also the `ossModelIdentity` is not present or it is not a valid value, the node cannot be synchronized.

This guide provides information on steps to identify and troubleshoot this issue.

Prerequisites

— Root access to the management server.

— Basic knowledge of Linux and JBoss.

— Basic knowledge of how to use the ENM CLI.

Steps

1. Verify that the node synchronization is activated and the sync status is UNSYNCHRONIZED. Execute the commands:

```
1)  cmedit get <NodeName> CmNodeHeartbeatSupervision.active
    FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)

2)  cmedit get <NodeName> CmFunction.syncStatus
    FDN : NetworkElement=<NodeName>,CmFunction=1
    syncStatus : UNSYNCHRONIZED

    1 instance(s)
```

2. Verify the nodeModelIdentity is not set executing the command:

```
cmedit get <NodeName> NetworkElement.nodeModelIdentity
FDN : NetworkElement=<NodeName>
nodeModelIdentity :

1 instance(s)
```

3. One of the reasons the nodeModelIdentity is not set is because the node is unreachable.

   To verify and troubleshoot this case, refer to *Node Unreachable from ENM* in

4. In case the node is reachable, verify if the Connectivity Information are correctly set in the node with the following command:

```
cmedit get NetworkElement=<NodeName>,SSRConnectivityInformation=1

FDN : NetworkElement=<NodeName>,SSRConnectivityInformation=1
snmpWriteCommunity : private
SSRConnectivityInformationId: 1
snmpSecurityName : null
snmpTrapPort : 162
snmpSecurityLevel : null
snmpReadCommunity : public
snmpAgentPort : 161
snmpVersion : SNMP_V2C
ipAddress : 10.44.107.115

1 instance(s)

cmedit get NetworkElement=<NodeName>,VREConnectivityInformation=1

FDN : NetworkElement=<NodeName>,VREConnectivityInformation=1
snmpWriteCommunity : private
VREConnectivityInformationId: 1
snmpSecurityName : null
snmpTrapPort : 162
snmpSecurityLevel : null
snmpReadCommunity : public
snmpAgentPort : 161
snmpVersion : SNMP_V2C
ipAddress : 10.44.107.115

1 instance(s)

cmedit get NetworkElement=<NodeName>,R8800ConnectivityInformation=1

FDN : NetworkElement=<NodeName>,R8800ConnectivityInformation=1
snmpWriteCommunity : private
R8800ConnectivityInformationId : 1
```

```
snmpSecurityName : null
snmpTrapPort : 162
snmpSecurityLevel : null
snmpReadCommunity : public
snmpAgentPort : 161
snmpVersion : SNMP_V2C
ipAddress : 10.44.107.115

1 instance(s)
```

5. If the the above parameters differs from the expected delete the Network element with the follwing commands:

```
cmedit action NetworkElement=<NodeName>,CmFunction=1 deleteNrmDataFromEnm

cmedit delete NetworkElement=<NodeName> -ALL --force
```

6. Create again the Network element with the following commands:

```
cmedit create NetworkElement=NESSR8004,SSRConnectivityInformation=1 SSRConne →
ctivityInformationId="1",transportProtocol="SSH",snmpAgentPort="161",ipAddre →
ss="192.168.102.44" -ns=SSR_MED -v=1.0.0
```

7. with the following commands set again the supervision to TRUE:

```
cmedit get <NodeName> CmNodeHeartbeatSupervision.active
FDN : NetworkElement=<NodeName>,CmNodeHeartbeatSupervision=1
    active : true

    1 instance(s)
```

Results

User understands the possible root causes of a node failing to synchronize with ENM the first time.

25 Integration of Network Element Software Store (CAS-C) with ENM

This section provides troubleshooting steps recommended to diagnose, and fix, common problems during the integration of Network Element Software Store (CAS-C) with ENM.

25.1 Troubleshoot ENM Connectivity issue with Network Element Software Store (CAS-C)

The first time ENM attempts to connect with the Network Element Software Store, it needs to set up some PIB parameters and also generate a key-pair value for authentification.

Possible Connectivity Issue Scenarios:

- ENM Connectivity with Network Element Software Store (CAS-C) Fails with Log Message- "Failed to connect to NeSoftwareStore with the Connectivity Information: Username=<username>, IP Address=<ipAddress>, Port=<sftpPort>".
- ENM Connectivity with Network Element Software Store (CAS-C) Fails with Log Message - "com.jcraft.jsch.JSchException: Auth fail".
- ENM Connectivity with Network Element Software Store (CAS-C) Fails with Log Message - "java.net.ConnectException: Connection refused: connect".

Prerequisites

- Root access to ENM Management Server (MS-1).
- Root login credentials for all VMs and Services of ENM physical.
- SHMSERV VM instance used for updating PIB parameters should be online.
- The key-pair files exist in the directory `/ericsson/tor/data/shm/sftp/`.
- The "Integration of Network Element Software Store (CAS-C) with ENM" workflow has been run.

Note: Refer to the section: *Integration of the CAS-C dropbox with ENM* of document [28] CAS Software Dropbox End-User Guide for instructions on how to integrate the Network Element Software Store (CAS-C) with ENM.

Steps

1. Verify the ENM PIB Parameters have the expected values.

   Note: Refer to the section: *Integration of the CAS-C Dropbox with ENM* of document [28] CAS Software Dropbox End-User Guide for instructions on how to integrate the Network Element Software Store (CAS-C) with ENM.

2. Verify generated public key onto Network Element Software Store (CAS-C)

   ```
   Private Key: [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sftp_key
   Public Key:  [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sftp_key.pub
   ```

   Note: If any key file is not generated, refer to section *Create the SSH key pairs* for details on how to read and update the connectivity information.

3. Verify the public key has been copied to Network Element Software Store (CAS-C).

   Note: Follow the instructions in section *Order access for ENM*, of document [28] CAS Software Dropbox End-User Guide.

4. If the issue persists, contact local Ericsson support.

25.2 Troubleshoot Package Download issue from Network Element Software Store (CAS-C)

25.2.1 Scenario: ENM Connectivity with Network Element Software Store (CAS-C) Fails with Log Message - "Import of Software Package '%s' from Ne Software Store failed.",13009, "Please check the logs for more details

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and Services of ENM physical.

— SHMSERV VM instance used for updating PIB parameters should be online.

— The key-pair files exist in the directory `/ericsson/tor/data/shm/sftp/`.

— The "Integration of Network Element Software Store (CAS-C) with ENM" workflow has been run.

Note: Refer to the section: *Integration of the CAS-C dropbox with ENM* of document [28] CAS Software Dropbox End-User Guide for instructions on how to integrate the Network Element Software Store (CAS-C) with ENM.

Steps

1. Verify the ENM PIB Parameters have the expected values.
    a. Perform the steps in Read Configurable Parameters for Network Element Software Store (CAS-C)
    b. If any PIB Parameter does not contain the correct value, refer to *Integration of the CAS-C dropbox with ENM* in document [28] CAS Software Dropbox End-User Guide for instructions on how to update the values.
2. Verify generated public key onto Network Element Software Store (CAS-C)

```
Private Key: [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sftp_key
Public Key:  [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sftp_key.pub
```

    Note: If any the keys files are not generated, please refer to *Create the SSH key pairs* step of *Integration of the CAS-C Dropbox with ENM* in document for details on how to read and update the connectivity information.
3. Verify the public key has been copied to Network Element Software Store (CAS-C).
    Note: Follow the instructions in section *Order access for ENM*, of document [28] CAS Software Dropbox End-User Guide.
4. Check if the CAS IP is online from MS-1.

```
[root @ms - 1 ~]# ping <CAS-IP>
```

5. Check if the packages are available in CAS server at location: `/data/Store/Deliverables`.
6. If the issue persists, contact local Ericsson support.

25.2.2 Scenario: During the Metadata Import or the Software Package Import, the Progress Stalls

The LVS Router either is offline or went offline during the import.

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and Services of ENM physical.

— The key-pair files exist in the directory `/ericsson/tor/data/shm/sftp/`.

— The "Integration of Network Element Software Store (CAS-C) with ENM" workflow has been run.

Note: Refer to the section: *Integration of the CAS-C dropbox with ENM* of document [28] CAS Software Dropbox End-User Guide for instructions on how to integrate the Network Element Software Store (CAS-C) with ENM.

Steps

1. Check to see that the LVS routers (`svc-1-lvsrouter` and `svc-2-lvsrouter`) are online, or have not faulted.

```
[root@svc]  hagrp -state | grep lvs
```

2. If either `svc-1-lvsrouter` or `svc-2-lvsrouter` are online, you can reschedule the metadata download, or reimport the software package.

    a. Bring the relevant service groups online.

    ```
    [root@svc] hagrp -online <Cluster> -sys <blade it is running on>
    ```

    b. Verify that at least one `lvs` router has come back online.

    Then reschedule the metadata download, or reimport the Software Package.

    ```
    [root@svc] hagrp -state | grep lvs
    ```

25.3 Troubleshoot Security issues with SSH Key-pair

25.3.1 Scenario: ENM Security with Network Element Software Store (CAS-C) Fails with Log Message- "bash: /ericsson/tor/data/shm/ne_software_store_configuration.bsh: No such file or directory"

The following instructions show how to copy the script `ne_software_store_configuration.bsh` in the directory: `/ericsson/tor/data/shm/`.

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and Services of ENM physical.

— SHMSERV VM instance used for updating PIB parameters should be online.

Steps

1. Verify if the script exists:

```
[root@ms-1 ~]# ls /ericsson/tor/data/shm/ne_software_store_configuration.bsh
```

2. If the script does not exist, run the following steps
    a. Access to the Management Server (MS-1).
    b. Get the SHMSERV VM information

```
[root@ms-1~]#  more /etc/hosts | grep shmserv
```

    c. Log on to SHMSERV VM using the following command:

```
[root@ms-1~]# ssh -i <enm_keypair.pem> cloud-user@svc-X-shmserv
```

    d. Verify that the script is on the shmserv VM's local file system:

```
[root@svc-X-shmserv~]# ls /ericsson/shm/ERICshmsoftwarepackagemanag →
ement_CXP9031632/etc/ne_software_store_configuration.bsh
```

    e. Copy the script to the shared file system:

```
[root@svc-X-shmserv~]# cp /ericsson/shm/ERICshmsoftwar →
epackagemanagement_CXP9031632/etc/ne_software_store_co →
nfiguration.bsh /ericsson/tor/data/shm/ne_software_sto →
re_configuration.bsh
```

    f. Verify script is copied across and has the correct access privileges:

```
[root@svc-X-shmserv~]# chown jboss_user:jboss /ericsso →
n/tor/data/shm/ne_software_store_configuration.bsh
[root@svc-X-shmserv~]# chmod 600 /ericsson/tor/data/sh →
m/ne_software_store_configuration.bsh
[root@svc-X-shmserv~]# ll /ericsson/tor/data/shm/ne_so →
ftware_store_configuration.bsh
```

Example of Expected Output:

```
-rw-------. 1 jboss_user jboss 12024 Sep 26 13:48 /ericsson/tor/dat →
a/shm/ne_software_store_configuration.bsh
```

25.4 Troubleshoot Setting the PIB parameters on ENM

25.4.1 Scenario: ENM Fails with Log Message - "Update [PIB_Parameter_Name] Parameter Failed. See Application Server Logs for Details"

Prerequisites

— Root access to the ENM Management Server (MS-1) is assigned.

— Root login credentials for all VMs and Services of ENM physical are assigned.

— The SHMSERV VM instance that is used for updating PIB parameters is online.

Steps

1. Verify that the ENM PIB Parameters have the expected values.
   — For instructions on integrating the Network Element Software Store (CAS-C) with ENM, see section: *Integration of the CAS-C Dropbox with ENM* of document [28] CAS Software Dropbox End-User Guide.
   — For instructions on integrating Instantaneous Licensing with ENM, see section *Integration of Instantaneous Licensing with ENM* of the document [8] ENM Configuration System Administrator Guide.
2. Contact local Ericsson support if any PIB Parameter does not have the expected value.

25.5 Troubleshoot Downloading Release Notes

25.5.1 Scenario: Downloading Release Notes for "Available for Import" Software Packages: ENM Fails with Log Message - "Cannot download release notes. Please try again"

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and services of ENM physical.

— SHMSERV VM instance used for updating PIB parameters must be online.

— CAS Server must be reachable from ENM MS-1.

Steps

1. Verify section Troubleshoot ENM Connectivity issue with Network Element Software Store (CAS-C) on page 228 is complete.

   The step corrects the connectivity issues from SHMServ to CAS.

2. If the issue persists, contact local Ericsson support.

25.5.2 Scenario: Downloading Release Notes for "Imported" Software Packages: ENM Fails with Log Message - "Cannot download release notes. Please try again"

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and Services of ENM physical.

— Software package downloaded in SMRS.

Steps

1. Verify the SHMServ VM is online.

```
[root@ms-1~]# cd /opt/ericsson/enminst/bin/
[root@ms-1~]# ./vcs.bsh --groups | grep shmserv
svc_cluster Grp_CS_svc_cluster_shmserv cloud-svc-2 standalone vm ONLINE OK -
```

2. Verify the SMRSserv VM is online.

```
[root@ms-1~]# cd /opt/ericsson/enminst/bin/
[root@ms-1~]# ./vcs.bsh --groups | grep smrs
svc_cluster Grp_CS_svc_cluster_smrsserv cloud-svc-1 standalone vm ONLINE OK -
```

3. Verify the availability of SMRS file system. Log into SHMServ and run the following command:

```
[root@ms-1~]# ssh -i /root/.ssh/vm_private_key cloud-user@svc-X-shmserv
[cloud-user@svc-X-shmserv ~]$ df -kh | grep smrs
10.144.64.17:/vx/ENM267-smrs 700G 1.9G 693G 1% /ericsson/tor/smrs
```

4. If the issue persists, contact local Ericsson support.

25.5.3 Scenario: ENM Has a Log Message - "Release Notes not found"

This is an `INFO` message, and no release note is present for the selected software package. Contact the respective node organization for additional information.

25.6 Troubleshoot Issues with CAS-C for Instantaneous Licensing

25.6.1 Scenario: ENM REST Client Fails to Connect to CAS-C. CAS Certificate Missing in SHMSERV Truststore

> On first-time connection to ENM, issues occur for one or both the following reasons:

— The PIB parameters for ENM Instantaneous Licensing do not have the expected values.

— No security certificate exists in ENM.

The error in full is as follows:

```
Sun.security.validator.ValidatorException: PKIX path building fa →
iled:

sun.security.provider.certpath.SunCertPathBuilderException: unab →
le to find valid certification path to requested target
```

Prerequisites

— Root access to the ENM Management Server (MS-1) is assigned.

— Root login credentials for all VMs and Services of ENM physical are assigned.

— The SHMSERV VM instance that is used for updating PIB parameters is online.

Steps

1. Get the SHMSERV VM information. If there is more than one SHMSERV VM, follow the process for all the VMs.

   ```
   [root@ms-1~]# more /etc/hosts | grep shmserv
   ```

2. Log on to SHMSERV VM using the following command:

```
[root@ms-1~]# ssh -i <enm_keypair.pem> cloud-user@svc-X-shmse →
rv
```

3. Change directory to `/ericsson/credm/data/certs/`.

```
[root@svc-X-shmserv~]#cd /ericsson/credm/data/certs/
```

4. Check if SHMSERV VM Truststore contains the CAS-C entry using the following command:

```
[root@svc-X-shmserv~ certs]# keytool -list -v -keystore shmIL →
-trustStore.jks
Enter keystore password: "athlone"
Owner: CN=<Owner-CN>, O=Ericsson, L=Budapest, C=HU
Issuer: CN=<Issuer-CN>, O=Ericsson, L=Budapest, C=HU
```

5. Check if the Common Name (CN) of the certificate matches the hostname in the REST request URL.

6. Contact the CAS operations team for the proper certificate if there is no match.

   For instructions on integrating Instantaneous Licensing with ENM, see section *Activation of Instantaneous Licensing in ENM* of the document [8] ENM Configuration System Administrator Guide

25.6.2 Scenario: ENM REST Client Fails to Connect to CAS-C - Host Name Does Not Match the Certificate Subject

The log message is as follows:

```
ERROR [com.ericsson.oss.services.shm.filestore.license.ilicense. →
impl.LicenseKeyF →
ileRequestHandler] (Thread-60 (HornetQ-client-global-threads-164 →
0693355)) Host n →
ame 'XXX.XXX.XX.XX' does not match the certificate subject provi →
ded by the peer →
(CN=XXXXX, OU=CAS, O=Ericsson, L=Budapest, ST=Budapest, C=HU)
```

Prerequisites

— Root access to ENM Management Server (MS-1).

— Root login credentials for all VMs and services of ENM.

— SHMSERV VM instance used for updating PIB parameters must be online.

Steps

1. Verify that the certificate is signed by the respective CAS-C. Check the owner and issuer of the certificate. Execute the command as follows:

```
[root@svc-X-shmserv~ certs]# keytool -list -v -keystore shmIL →
-trustStore.jks
Enter keystore password: "athlone"
Owner: CN=<Owner-CN>, O=Ericsson, L=Budapest, C=HU
Issuer: CN=<Issuer-CN>, O=Ericsson, L=Budapest, C=HU
```

2. Check if the Common Name (CN) of the certificate matches the hostname in the REST request URL. Contact the CAS operations team for the proper certificate if there is no match.

   Note: Hostname and IP address cannot be used interchangeably. If URL used is IP-based, then certificate must show IP and vice versa.

3. Execute the following steps to update the **SAN** field with IP Address, if the CAS-C certificate is issued by ENM:

   — Edit the **Certificate Profile** created for CAS-C in PKI Profile Management.

   — Navigate to **Extensions > Capabilities tab > Subject Alternative Name** and select the **IP address** option from the drop down.

   — Edit the **End Entity** and provide the IP address of CAS-C for the **Subject Alternative Name** field in PKI Entity Management and click **Submit**.

   — Use the updated **End Entity** to issue the certificate for the CAS-C key store and install new certificates on CAS-C.

25.6.3 Scenario: ENM REST Client Fails with "unSupported_certificate" or "unsupported certificate purpose" Error

This issue is applicable if the ENM CA is subtended to an external CA and ENM is issuing certificates to CAS-C.

When ENM CA is subtended to external CA, make sure that the signed certificate for ENM_PKI_Root does not contain the EnhancedkeyUsage (for example, securemail), AuthorityInformationAccess, and SubjectAlternateName fields.

25.6.4 Scenario: ENM REST Client Fails With an Error Message: "request" Activity Failed. Failure Reason: SFTP Key File does not Exist. Please Check CAS-C SWDX SSH Keys Configuration

> This occurs when the SFTP Keys configuration is incorrect in ENM.

The error is as follows:

```
Sending License Request Failure to node with values as : {NODE_N →
AME=<NODENAME>, requestType=LKF_REFRESH, errorCategory=null,

requestId=null, resultCode=MESSAGE_ERROR, cxcList=null,

requestInfo=SFTP Key file does not exist. Please check CAS-C SWD →
X SSH keys configuration., id=6}
```

Prerequisites

- Root access to the ENM Management Server (MS-1) is assigned.
- Root login credentials for all VMs and Services of ENM physical are assigned.

Steps

1. Verify generated public key onto Network Element Software Store (CAS-C).

   ```
   Private Key: [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sft →
   p_key
   Public Key: [root@ms-1~]# ls /ericsson/tor/data/shm/sftp/sftp →
   _key.pub
   ```

   Note: If any key file is not generated, refer to section *Create the SSH key pairs* for details on how to read and update the connectivity information.

2. Verify that the public key has been copied to Network Element Software Store (CAS-C).

   Note: Follow the instructions in section *Order access* for ENM, of document [28] CAS Software Dropbox End-User Guide

3. If the issue persists, contact local Ericsson support.

25.6.5 Scenario: ENM Fails to Find LKF Packages with log Message " Could not change to SFTP directory : %s"

> This can occur when ENM could not change the path of Software Dropbox Directory and so ENM failed to find the LKF Packages.

Prerequisites

— Root access to the ENM Management Server (MS-1) is assigned.

— Root login credentials for all VMs and Services of ENM physical are assigned.

— SHMSERV VM instance used for updating PIB parameters must be online.

Steps

1. Check if the Software Dropbox Directory Path is correctly configured.

   Note: The path `%s`, must be the value from the `INSTANTANEOUS_LICENSE_SOFTWARE_DROPBOX_DIRECTORY_PATH`.

2. Check if the packages are available in CAS-C server at location: `%s`.

3. If the issue persists, contact local Ericsson support.

25.6.6 Scenario: ENM REST Client fails with an error message: "request" activity failed. Failure Reason : HTTP/1.1 400 Bad Request

This error occurs when the HTTPS REST request sent to ELIS/CAS is incorrect. A request may be incorrect if it is missing a parameter or has a malformed request payload. This is an application-level error message which means that the server is running correctly and is able to listen to the incoming traffic (REST Request) at the specified TCP port.

Prerequisites

ENM is configured properly.

Steps

1. Verify that the PIB parameters are configured correctly.

   For instructions on integrating Instantaneous Licensing with ENM, see the *Activation of Instantaneous Licensing in ENM* section of the [8] ENM Configuration System Administrator Guide.

2. If the issue persists, contact CAS support.

Note: Additional information about the possible cause of this error is present in the error message.

25.6.7 ENM REST Client fails with an error message: "request" activity is failed. Failure Reason : ENM is not able to connect to CAS-C

> This error occurs when CAS-C services are not responding properly. This is a server-level error message which means that the servers are not in a position to serve the desired request.

The error is as follows:

```
Sending License Request Failure to node with values as :

{NODE_NAME=<NODE NAME>, requestType=LKF_REFRESH, errorCategory=n →
ull,

requestId=null, resultCode=CAS_NOT_REACHABLE, cxcList=null, requ →
estInfo=ENM is not able to connect to CAS-C, id=4}
```

Prerequisites

— ENM is configured properly.

— Execute the following command to check if CAS SPC is listening to the incoming HTTPS traffic on the specified traffic. Execute this command from any of the ENM server or VM.

```
nc -z -v <INSTANTANEOUS_LICENSE_SENTINEL_PROXY_IP_ADDRESS> <INSTANTANEOUS_LICENSE_SEN →
TINEL_PROXY_PORT_NUMBER>
```

Note: `INSTANTANEOUS_LICENSE_SENTINEL_PROXY_IP_ADDRESS` and `INSTANTANEOUS_LICENSE_SENTINEL_PROXY_PORT_NUMBER` are PIB parameters for which the values are provided by CAS operations.

Steps

1. Verify that the PIB parameters are configured correctly.

   For instructions on integrating Instantaneous Licensing with ENM, see the *Activation of Instantaneous Licensing in ENM* section of the [8] ENM Configuration System Administrator Guide.

2. If the issue persists, contact CAS support.

25.6.8 ENM REST Client fails with an error message: "request" activity is failed. Failure Reason : CAS-C is not able to connect to CAS-E

> This error occurs when CAS-C to CAS-E connectivity fails.

This is a server-level error message which means that the servers are not in a position to serve the desired request.

The error is as follows:

```
Sending License Request Failure to node with values as :

{NODE_NAME=<NODE NAME>, requestType=LKF_REFRESH,

errorCategory=null, requestId=null, resultCode=ECN_CONNECTION_ER →
ROR, cxcList=null, requestInfo=CAS-C is not able to connect to C →
AS-E, id=1}
```

Please contact CAS support with the error details.

25.6.9 ENM REST Client fails with an error message: "request" activity is failed. Failure Reason : CAS-E is not able to connect to ELIS

> This error occurs when CAS-E to ELIS connectivity fails.

This is a server-level error message which means that the servers are not in a position to serve the desired request.

The error is as follows:

```
Sending License Request Failure to node with values as :

{NODE_NAME=<NODE NAME>, requestType=LKF_REFRESH,

errorCategory=null, requestId=null, resultCode=ELIS_CONNECTION_E →
RROR, cxcList=null, requestInfo=CAS-E is not able to connect to  →
ELIS, id=1}
```

Please contact CAS support with the error details.

26 Auto Provisioning Troubleshooting

This section provides the troubleshooting information required to diagnose and fix common problems when running AutoProvisioning activities.

The following table lists the AutoProvisioning tasks related to node auto integration that may require troubleshooting.

Table 10 Auto Provisioning Tasks

Node Type	Task	Progress	Troubleshooting Resolution
ERBS	Node Up Notification	Waiting	Waiting for Node Up (ERBS) on page 246
All	Node Synchronization Notification	Waiting	Check Synchronization of the Node on page 246
ERBS	Activate Optional Features	Failed	Check Optional Features (ERBS) on page 246
RadioNode Router6672 Router6675 Router6x71	Create Backup	Failed	Check Backup on page 247
ERBS	Create CV	Failed	Check Backup on page 247
RadioNode Router6672 Router6675 Router6x71	Upload Backup	Failed	Check Backup on page 247
ERBS	Upload CV	Failed	Check Backup on page 247
RadioNode MSRBS_V1	Import Configurations	Failed	Check Import Errors on page 247

Node Type	Task	Progress	Troubleshooting Resolution
MSRBS_V1	Ready for Service Notification	Failed	Pico Notifications (MSRBS_v1) on page 247
ERBS	Initiate Import Configurations	Failed	Check Import Errors on page 247
ERBS	Site Config Complete Notification	Waiting	Task 'Site Config Complete Notification' Remains at Waiting (ERBS) on page 260
ERBS	S1 Complete or S1 Not Needed Notification	Waiting	Node Notifications Issues (ERBS) on page 248
ERBS	Unlock Cells	Failed	Check Unlock Cells on page 248
All	Validate Configuration	Failed	Validate Configuration Issues on page 248
RadioNode	Node Downloading Configurations	Failed	Issues with Node Downloading Configurations on page 249
RadioNode	Node Installing Configurations	Failed	Issues with Node Installing Configurations on page 249
RadioNode	Node Sending Node Up	Failed	Node Sending Node Up Task Remains at Started Status on page 249
RadioNode	Configure Software Management	Failed	Configure Software Management on page 250
MSRBS_V1	Generate Security	Failed	Security Generation Issues on page 250

The following table lists the hardware replace tasks that may require troubleshooting.

Table 11 Hardware Replace Tasks

Node Type	Task	Progress	Troubleshooting Resolution
MSRBS_V1	Node Up Notification	Waiting	Hardware Replace 'Node Up Notification' Task Remains at Waiting (MSRBS_v1) on page 251
MSRBS_V1	Node Synchronization Notification	Waiting	Hardware Replace Node Synchronization (MSRBS_v1) on page 251
MSRBS_V1	Configure DHCP	Failed	Hardware Replace DHCP Configuration on page 251
MSRBS_V1	Remove DHCP Client Configuration	Failed	Hardware Replace DHCP Configuration on page 251
Radio Node	Generate Security	Failed	Hardware Replace Generate OssNodeProtocol Failure on page 252

The following table lists the expansion tasks that may require troubleshooting.

Table 12 Expansion Tasks

Node Type	Task	Progress	Troubleshooting Resolution
RadioNode	Restore Backup	Failed	Expansion Backup Issues on page 253
RadioNode	Expansion Notification	Waiting	Expansion Notification Issues on page 252

Node Type	Task	Progress	Troubleshooting Resolution
RadioNode	Import Configuration	Failed	Expansion Import Configurations Issues on page 252

The following table lists general Auto Provisioning issues and troubleshooting scenarios that can be used to identify and resolve the issues.

Table 13 Auto Provisioning Issues and Troubleshooting Scenarios

Node Type	Task	Troubleshooting Resolution
All	Email fails to deliver	AutoProvisioning Email Issues on page 254
All	Completed Nodes or Projects disappear	Projects Housekeeping on page 295
All	AP Delete Failed	Auto Provisioning Deletion Issues on page 253
RadioNode	Node Integration Status Entries are not updating in LMT scenario	Auto Provisioning Node Integration Status Tasks Not Appearing for LMT Integration on page 254

26.1 Troubleshooting Resolution

This section outlines the troubleshooting resolutions and multiple steps to help identify and resolve issues that may arise when executing Auto Provisioning activities.

26.1.1 Node Integration Troubleshooting

This section describes how to troubleshoot a node that fails to integrate successfully or is paused during Integration.

Target Groups

To execute node integration, you must have the following role:

— Autoprovisioning_Operator

The following are some common scenarios that may require additional troubleshooting:

26.1.1.1 Waiting for Node Up (ERBS)

> For automatic integration of a node with ENM, Auto Provisioning stores the configuration files for retrieval by the node. The node retrieves these files once it is turned on, installs them, and then send a `Node Up Notification` to ENM to inform ENM that all the configuration files have been installed.

The following is a list of troubleshooting steps:

— Task 'Node Up Notification' Progress Remains at Waiting (ERBS) on page 255

— Node Cannot Find the Interfaces Published on CORBA Southbound Naming Service (ERBS) on page 256

— Node Cannot Find the CORBA Southbound Naming Service (ERBS) on page 258

26.1.1.2 Check Synchronization of the Node

> For automatic integration of a node with ENM, Auto Provisioning automatically starts node synchronization after a Node Up Notification. The node sends a `Node Up Notification` to inform ENM that it's O&M (Operation and Maintenance) connectivity is configured.

Synchronization issues may arise due to issues such as configuration and connectivity, the following steps outline additional steps to troubleshoot synchronization:

— Task 'Node Synchronization Notification' Remains at Waiting on page 267

26.1.1.3 Check Optional Features (ERBS)

> The `Activate Optional Features` task activates the optional features defined by the LKF. It is executed once all the configurations have been applied to the node and when the activate license is set to true in the node information file.

To troubleshoot failure related to activate options features perform the following troubleshooting steps:

— Task 'Activate Optional Features' is Failed (ERBS) on page 264

26.1.1.4 Check Backup

> During node integration, Auto Provisioning creates backups and configuration versions (CV) at various stages of the integration process. This allows a customer to revert to an earlier version of the node if an issue arises during auto integration. Upload of the backup to ENM is also supported, dependent on node type this is optional or mandatory.

To troubleshoot backup issues the following troubleshooting steps are recommended:

— Tasks 'Create CV or 'Upload CV' Failures (ERBS) on page 265

— Tasks 'Create Backup' or 'Upload Backup' Failures on page 266

26.1.1.5 Check Import Errors

> Post node synchronization, additional configuration files are applied to the node. These can be in Bulk CM, NETCONF (Baseband Radio Node) or amos (Baseband Radio Node) format. The pushing of these files to the node are represented by the Import Configuration (Initiate Import Configuration and Unlock Cells for ERBS) task.

To troubleshoot import configuration errors the following troubleshooting steps are recommended:

— Task 'Import Configurations' is Failed on page 261

— Task 'Initiate Import Configurations' is Failed (ERBS) on page 263

26.1.1.6 Pico Notifications (MSRBS_v1)

> Pico node (MSRBS_V1) is a COM/ECIM based node and certain tasks in the Auto Integration process are triggered by the node updating it's MOM parameters. The node MO NodeFunction attribute `rbsConfigLevel` is one of the parameters used to drive the Auto Integration process on pico nodes.

If the Radio Network Configuration procedure on the node fails, for example, by S1-link establishment failure, the node will not set `RbsConfigLevel` to `READY_FOR_SERVICE`. Instead the node will set the `RbsConfigLevel` to `AI_RNW_CONFIGURATION_FAILED` to indicate the failure to AP.

To troubleshoot pico errors around notifications the following troubleshooting steps are recommended:

— Task 'Ready For Service Notification' is Failed (MSRBS_v1) on page 268

26.1.1.7 Node Notifications Issues (ERBS)

> DU Radio Node (ERBS) is a CPP based node and certain task in the Auto Integration process are triggered by the node updating its MOM parameters. The Node MO RbsConfiguration attribute `rbsConfigLevel` is one of these parameters used to drive the Auto Integration process.

Issues may arise with notifications of state change not triggering continuation of the AutoProvisioning flow the following troubleshooting steps outline how to fix these issues:

— Task 'Site Config Complete Notification' Remains at Waiting (ERBS) on page 260

— Task 'S1 Complete or S1 Not Needed Notification' Remains at Waiting (ERBS) on page 261

26.1.1.8 Check Unlock Cells

> Auto Provisioning supports automatic unlocking of cells as part of the Auto Integration flow. For DU Radio Nodes (ERBS) this is represented as an additional task in the AP node status output called unlock cells. For Baseband Radio Nodes this is executed as part of the Import configurations task. The Unlock cells task applies the content of a bulk cm file (also NETCONF for Baseband Radio Node) that is referenced in the unlock cells tag in the node information file.

Issues may arise with the unlocking of cells the following troubleshooting steps outline how to fix these issues:

— Task 'Unlock Cells' is Failed (ERBS) on page 265

26.1.1.9 Validate Configuration Issues

> When an Auto Integration is executed against configurations that are built as part of the Add Node or from pre-create Auto Provisioning project, there is a range of validation that is executed against the input files.

Validation failures can occur for several reasons. The following troubleshooting steps outline how to fix these issues:

— Task 'Validate Configuration' Unable to Validate NETCONF Files (Radio Node) on page 268

26.1.1.10 Issues with Node Installing Configurations

> As part of Node Integration, the node sends status information to AP via the AIWS (Auto Integration Web Server) interface. This task shows progress information around the node installing the configuration files that were retrieved from the SMRS, such as the `SiteBasic`, `SiteEquipment`, and `OssNodeProtocol` file.

Issues can occur due to several reasons. The following troubleshooting steps outline how to fix these issues:

— Upload Fixed Site Basic and Wait for Next Run of Integration on page 270

— Collect Node Logs on page 290

26.1.1.11 Issues with Node Downloading Configurations

> As part of Node Integration the node sends status information to AP via the AIWS (Auto Integration Web Server) interface. This task show progress information around the node downloading the configuration files from the SMRS.This error may be due to an issue with the Upgrade Package or an issue with configuration files downloaded from the SMRS, such as `OssNodeProtocol`, `SiteBasic`, `RbsSummary` and `SiteEquipment` file.

Issues can occur due to several reasons. The following troubleshooting steps outline how to fix these issues:

— Upgrade Package Deleted in SHM on page 271

— Fix Configuration Files on page 270

26.1.1.12 Node Sending Node Up Task Remains at Started Status

> The **Node Sending Node Up Task** task remains in **Started** status if there is an issue with the Node to ENM connection or for some reason the node messages are not sent in the correct sequence. If the **Node Up Notification** task is **Received** and the **Sending Node Up** task remains in **Started**, then there is no impact to node integration except the status reporting.

Issues can occur due to several reasons. The following troubleshooting steps outline how to fix these issues:

— Rectify AIWS Port Configurations on page 272

— Collect Node Logs for Baseband Radio Node on page 291

26.1.1.13 Configure Software Management

> The configure software management task enables node support for Hardware Sensitive Install (HSI). As part of this task, AP automatically generates a machine to machine user and password that is set on the SwM MO of the node. The machine to machine user and password allows the node to access the upgrade package from the SMRS of ENM.

Note: Failing to configure software management does not impact auto-integration. However, it results in the node not being correctly configured for HSI.

If the configure software management task fails, execute the steps mentioned in Configure Software Management Task Fails to Update SwM MO on page 272.

26.1.1.14 Security Generation Issues

> During Security Generation, AP generates required security artifacts and sets up the nodes security requirements within ENM.

The following is a troubleshooting step that can support resolving issues that may arise when AP is executing the Generate Security Task:

— Task 'Generate Security' Fails on page 286

26.1.2 Hardware Replace Troubleshooting

> This section describes how to troubleshoot issues that may arise when executing Hardware Replace using Auto Provisioning.

Target Groups

To execute hardware replace, you must have the following role:

— Autoprovisioning_Operator

The following are some common scenarios that may require additional troubleshooting:

26.1.2.1 Hardware Replace 'Node Up Notification' Task Remains at Waiting (MSRBS_v1)

> Zero Touch Hardware replace, for MSRBS_v1 (pico) sends a Node Up Notification to ENM to inform ENM that all the replacement configuration has been applied to the node and the O&M configuration has been successfully established. The Node Up Notification is sent as an SNMP trap.

The following is a list of troubleshooting steps to support identifying issues that may cause a hardware replace to be stuck in waiting for the "Node Up Notification":

— Hardware Replace 'Node Up Notification' Remains at Waiting (MSRBS_v1) on page 273

26.1.2.2 Hardware Replace Node Synchronization (MSRBS_v1)

> Hardware replace, for pico (MSRBS_v1) sends a Node Up Notification to ENM to inform ENM that all the replacement configuration has been applied to the node and the O&M configuration has been successfully established. The Node Up Notification is sent as an SNMP trap and Auto Provisioning starts node synchronization.

The following is a list of troubleshooting steps to support identifying issues that may cause a hardware replace to be stuck in waiting for the `Node Synchronization`:

— Hardware Replace 'Node Synchronization Notification' Remains at Waiting (MSRBS_v1) on page 274

26.1.2.3 Hardware Replace DHCP Configuration

> As part of AutoProvisioning Zero Touch, Hardware replace Auto Provisioning automatically configures the ENM DHCP with the required network configuration to support Zero Touch hardware replace.

The following is a troubleshooting step that can support resolving issues that may arise during hardware replace around DHCP configuration:

— Hardware Replace 'Configure DHCP' or 'Remove DHCP Client Configuration' is Failed on page 276

26.1.2.4 Hardware Replace Generate OssNodeProtocol Failure

> As part of Baseband Radio Node Hardware Replace Auto Provisioning generates provisioning artifacts that are required for the replacement to retrieve when it is being added to ENM

The following is a troubleshooting step that can support resolving issues that may arise when AP is executing the Generate Security Task:

— Generate Security Fails due to Unsupported Configuration on page 278

26.1.3 Node Expansion Troubleshooting

> This section describes how to troubleshoot issues that may arise during node expansion when executed through Auto Provisioning.

Target Groups

To execute node expansion, you must have the following role:

— Autoprovisioning_Operator

26.1.3.1 Expansion Notification Issues

> Auto Provisioning Expansion requires a notification from the node or by an ENM Operator executing ap resume to indicate that the hardware related activity for node expansion has been completed. The field technician can trigger the node notification by pressing the **Maintenance** button when beginning the Expansion activity and then pressing it again when the activity is completed.

The following is a list of troubleshooting steps to support identifying issues that may occur around the expansion notification:

— Expansion Notification Task Remains at Waiting Status on page 279

26.1.3.2 Expansion Import Configurations Issues

> Configuration files applied to the node can be in Bulk CM format , NETCONF (Baseband Radio Node) or amos (Baseband Radio Node) format. The

> pushing of these files to the node are represented by the Import Configuration task.

The following is a list of troubleshooting steps to support identifying issues that may occur around the expansion import configurations:

— Expansion Task 'Import Configurations' is Failed on page 281

26.1.3.3 Expansion Backup Issues

> As part of the expansion flow, Auto Provisioning can restore a node to a previously created backup.

The following is a list of troubleshooting steps to support identifying issues that may occur around restoring a node to a previously created backup during the expansion flow:

— Restore Backup Task Remains at Started on page 283

26.1.4 General Auto Provisioning Troubleshooting

> This section outlines issues that may occur when executing Auto Provisioning activities that are not specific to any task or use-case.

26.1.4.1 Auto Provisioning Deletion Issues

If a user executes a delete in auto provisioning the behavior varies dependent on several factors.

— The use-case (auto integration, hardware replace, expansion or reconfiguration)

— The state of the workflow, such as Integration failed, Order Completed, and so on.

— Node Synchronization and Heartbeat supervision state.

Auto Provisioning delete for node integration executes the following for incomplete integrations:

— Any active workflow instances for the node are canceled and deleted.

— Any security entities (if security was generated) are canceled and deleted and the network element is removed.

Note: This execution is dependent on the Auto Integration activity and the state. If a Network Element is synchronized, or has the MO CmNodeHeartBeatSupervision attribute active set to true the Network Element will not be removed.

— Any AP-generated artifacts are deleted.

— The AP node MO is deleted (and the AP project MO is also deleted, if no nodes or profiles remain in the project).

If a node integration completes successfully the Network Element is not removed.

The network element is not removed for hardware replace, expansion or reconfiguration.

The following is a list of troubleshooting steps to support identifying issues that may occur around the auto provisioning node data deletions:

— Task 'Cancel Security' Fails on page 284

26.1.4.2 AutoProvisioning Email Issues

> Auto Provisioning supports the sending of email with the auto provisioning status output.

The following is a list of troubleshooting steps to support identifying issues that may occur around emails not being sent:

— Email with Node Status Fails to Deliver on page 285

26.1.4.3 Auto Provisioning Node Integration Status Tasks Not Appearing for LMT Integration

> As part of Node Integration, the node sends status information to AP via the AIWS (Auto Integration Web Server) interface.

Note: For LMT Integration, the node logical name must be included in the `Site Installation` file for node status entries to be shown in the Auto Provisioning node status output.

Issues can occur with the visibility of the node status tasks. The following troubleshooting steps outline how to fix these issues:

— Rectify AIWS Port Configurations on page 272

26.2 Auto Provisioning Resolutions

This section describes the steps to resolve issues that may arise during execution of the Auto Provisioning activities.

Note: The troubleshooting steps described below are based on a physical ENM deployment. Different ENM deployments, such as cloud may have slightly different service group naming or directory naming. Please see the deployment specific documentation for variations.

26.2.1 Automatic Node Integration Troubleshooting Steps

This section describes the steps to resolve the issues that may arise during execution of node auto integration.

26.2.1.1 Task 'Node Up Notification' Progress Remains at Waiting (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Scripting Operator

— Node access

Steps

1. Confirm the scenario:

    a. Check that "Node Up Notification" task is still at Waiting in Auto Provisioning Node status output.

    ```
    ap status -n <nodeName>
    ```

    b. Check the Autointegration_report.log from node logs to confirm that the node up message has been sent successfully.

    For more information on these logs, see Collect Node Logs for DU Radio Node (ERBS) on page 290

2. Get Visinaming-Southbound IP address:

    a. Logon to Shell Terminal on Scripting.

For more information, refer to Collect ENM Logs on page 288.

b. Check the IP addresses (IPv4 and IPv6) of `visinaming-sb` global.properties file

```
[<username>@scp-1-scripting(enmHost) ~]$ cat /ericsson/tor/data/global.properties  | grep visinamingsb_service
```

```
visinamingsb_service_IPv6_IPs=<ipv6-ipaddress>
```

```
visinamingsb_service_IPs=<ipv4-ipaddress>
```

3. Confirm the `ossCorbaNameServer` value in SiteBasic file:

   a. Download the imported artifacts using ENM CLI (or AutoProvisioning UI using LMT Download)

   ```
   ap download -i -n <nodeName>
   ```

   b. Check the value of '`ossCorbaNameServer`' in the downloaded `siteBasic.xml`

4. If the value retrieved from the siteBasic.xml does not match the value retrieved from the global.properties file:

   a. Delete the ordered node using ENM CLI (or AutoProvisioning UI delete).

   ```
   ap delete -n <nodeName>
   ```

   b. Delete all nodes excluding the node with the faulty `siteBasic.xml` in the original project zip file.

   c. In the node configuration data in the project zip file, update the value of '`ossCorbaNameServer`' in the `siteBasic.xml` (with the value retrieved from step 3.b).

   d. Reorder the project with the node containing the correct information.

   ```
   ap order file:<project.zip>
   ```

26.2.1.2 Node Cannot Find the Interfaces Published on CORBA Southbound Naming Service (ERBS)

Prerequisites

— You must have access to connect to a virtual machine. For more information, see Connect to a Virtual Machine on page 2

— Node Access

Steps

1. Confirm the scenario:

    a. Check that the `Node Up Notification` task is still at `Waiting` in the Auto Provisioning Node status output.

    ```
    ap status -n <nodeName>
    ```

    b. Open the node `configurationReport log`.

    For more information, refer to Collect Node Logs for DU Radio Node (ERBS) on page 290.

2. To verify the error, search the log file for the following exception message:

    ```
    org.omg.CosNaming.NamingContextPackage.NotFound: IDL:omg.org/CosNaming/Namin
    gContext/NotFound:1.0
    ```

3. Force the publication of services interfaces on CORBA naming service by restarting the JBoss service on MSAP VMs.

    Note: This is an intrusive action and may result in performance degradation.

    This need to be done on all `MSAP` VMs (`msap` on `svc-1`, `svc-2` and so on.)

    a. Enable debug. To verify that the command has been successful, change the Node Discovery log level to DEBUG:

    ```
    [root@svc-1-msap ~]# /ericsson/3pp/jboss/bin/jboss-cli.sh --connect
    jboss-cli > /subsystem=logging/logger=com.ericsson.oss.mediation.no
    dediscovery:add(level=DEBUG)
    ```

    Result: The following indicates that the operation was successful:

    ```
    {"outcome" => "success"}
    ```

    b. Restart the JBoss service:

    ```
    [root@svc-1-msap ~]# service jboss restart
    ```

    Result: A series of messages are displayed. The most recent ones are similar to the following:

    ```
    jboss-as is running
    JBOSS: INFO (): Run post-start scripts
    JBOSS: INFO (): JBoss execute script as background process : /erics
    son/3pp/jboss/bin/post-start/configure_share_permissions.sh
    ```

```
JBOSS: INFO (): JBoss execute script as background process : /erics
son/3pp/jboss/bin/post-start/mediation_config.py
                                                          [  OK  ]
```

4. Check if the services interfaces were properly bound to CORBA naming service:

    a. Search on JBoss logs for following message, using the tail and grep tools:

    ```
    [root@svc-1-msap ~]# tail -n 2000 /ericsson/3pp/jboss/standalone/lo
    g/server.log | grep 'Successfully bound CORBA object to path'
    ```

    Result: The results are similar to the text below. Make sure the time and date matches with the current date.

    ```
    2015-05-29 10:57:03,478 DEBUG [com.ericsson.oss.mediation.nodedisco
    very.naming.NameServiceMonitor] (Thread-0 (HornetQ-client-global-th
    reads-51813064)) Successfully bound CORBA object to path com/ericss
    on/nms/umts/ranos with name WmaNodeDiscovery.
    2015-05-29 10:57:11,509 DEBUG [com.ericsson.oss.mediation.nodedisco
    very.naming.NameServiceMonitor] (Thread-0 (HornetQ-client-global-th
    reads-51813064)) Successfully bound CORBA object to path com/ericss
    on/nms/umts/ranos with name WmaNodeDiscoveryUnsecure.
    2015-05-29 10:57:11,541 DEBUG [com.ericsson.oss.mediation.nodedisco
    very.naming.NameServiceMonitor] (Thread-0 (HornetQ-client-global-th
    reads-51813064)) Successfully bound CORBA object to path com/ericss
    on/nms/umts/ranos with name WmaNodeSecurity.
    2015-05-29 10:57:11,584 DEBUG [com.ericsson.oss.mediation.nodedisco
    very.naming.NameServiceMonitor] (Thread-0 (HornetQ-client-global-th
    reads-51813064)) Successfully bound CORBA object to path com/ericss
    on/nms/umts/ranos with name WmaNodeSecurityUnsecure.
    ```

5. In order to avoid excess entries on JBoss logs, change the Node Discovery log level back to INFO:

    ```
    [root@svc-1-msap ~]# /ericsson/3pp/jboss/bin/jboss-cli.sh --connect
    jboss-cli > /subsystem=logging/logger=com.ericsson.oss.mediation.nodediscove
    ry:change-log-level(level=INFO)
    ```

    Result: The following indicates that the operation was successful:

    ```
    {"outcome" => "success"}
    ```

26.2.1.3 Node Cannot Find the CORBA Southbound Naming Service (ERBS)

Prerequisites

— You must have access to connect to a virtual machine. For more information, see Connect to a Virtual Machine on page 2

— Node Access

Steps

1. Confirm the scenario:

    a. a. Check that "Node Up Notification" task is still at Waiting in Auto Provisioning Node status output.

    ```
    ap status -n <nodeName>
    ```

    b. Open the node `configurationReport log`.

    For more information, refer to Collect Node Logs for DU Radio Node (ERBS) on page 290.

    c. Search the log file for the following exception message:

    ```
    org.omg.CORBA.COMM_FAILURE:   vmcid: SUN  minor code: 201  complete
    d: No
    ```

    If the entry was found, there are two paths to follow: check if southbound naming service is running and check if the firewall is properly configured.

2. Check if southbound naming service is running.

    a. Connect to the `visinaming-sb` VM.

    b. Check the `visinaming-sb` service status:

    ```
    [root@visinamingsb ~]# service visinaming-sb status
    ```

    Result: The following message indicates that the service is running, any other result indicates a problem.

    ```
    (pid  XXXX) is running...
    ```

    c. Start the `visinaming-sb` service.

    ```
    [root@visinamingsb ~]# service visinaming-sb start
    ```

    Check the status (step 1) after starting the service.

3. Check if the firewall is properly configured

    a. Node Discovery uses the ports `50073, 50340 and 50341` for secure and unsecured communication with the node, so they should be opened on ENM master server firewall.

    It can be verified using `iptables` command.

```
[root@svc-1 ~]# iptables -S | grep -E '(50073|50340|50341)'
```

Result: The following message indicates that the firewall is properly configured, any other result indicates an issue.

Proceed to next step and create the firewall rules.

b. Create the firewall rules for Node Discovery.

```
[root@svc-1 ~]# iptables -A INPUT -p tcp -m multiport --dports 5007 →
3,50340,50341 -m comment --comment "019 nodediscovery tcp" -m state →
 --state NEW -j ACCEPT
[root@svc-1 ~]# iptables -A OUTPUT -p tcp -m multiport --dports 500 →
73,50340,50341 -m comment --comment "019 nodediscovery tcp" -m stat →
e --state NEW -j ACCEPT
```

26.2.1.4 Task 'Site Config Complete Notification' Remains at Waiting (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Node access

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status `Site Config Complete Notification` task is stuck at waiting.

2. Verify node Synchronization:

    a. Check if there was a problem during Node Synchronization. For more information, see CM Node Synchronization Troubleshooting - CPP Based Nodes on page 47

3. Check the `Autointegration_report.log` from node logs to confirm that the RbsConfiguration attribute `RbsConfigLevel` has been set to `SITE_CONFIG_COMPLETE`.

    For more information, see Collect Node Logs for DU Radio Node (ERBS) on page 290.

26.2.1.5 Task 'S1 Complete or S1 Not Needed Notification' Remains at Waiting (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Node access

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status `S1 Completed or S1 Not Needed Notification` task is stuck at waiting.

2. Verify node Synchronization:

    a. Check if there was a problem during Node Synchronization. For more information, see CM Node Synchronization Troubleshooting - CPP Based Nodes on page 47

3. Check the `Autointegration_report.log` from node logs to confirm that the RbsConfiguration attribute `RbsConfigLevel` has been set to `S1_COMPLETE` or `S1_NOT_NEEDED`.

    For more information, see Collect Node Logs for DU Radio Node (ERBS) on page 290.

26.2.1.6 Task 'Import Configurations' is Failed

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output indicates that `Import Configuration` task is failed, and the overall state is in integration suspended.

    b. Note any additional information in the `ap` node status output for the failing task.

2. Fix the file that has the reported issues and retry.

    a. For BULK CM file, the job ID is provided. Examine the output job verbose output:

        i. Open ENM CLI.

        ii. Run the following command:

        ```
        cmedit import --status --job <Job_ID> --verbose
        ```

        iii. Examine the verbose output of the Job ID.

        iv. If the reason for the import failure can be identified from the verbose import job status output, you can update the file that is causing the issue.

    b. For NETCONF file, the job ID is not provided. Examine the ap node status output:

        i. Check the Message ID in the error messages of additional information, find the corresponding edit-config rpc in the file. If the Message ID is in the format of `message-id is unknown, the rpc edit-config message sequence is #<sequence>`, count the edit-config rpc in the file and locate the failed rpc according to the sequence.

        ii. If the reason for the import failure can be identified from additional information in the ap node status output, you can update the file that is causing the issue.

    c. For amos file, the job ID is not provided. Examine the ap node status output:

        i. Click the `<contextual link>` in additional information then check AMOS contextual log for details.

        ii. If the reason for the import failure can be identified from additional information in the ap node status output, you can update the file that is causing the issue.

Note:
- To access the `<contextual link>`, you need to have Scripting_Operator role.
- Due to limitation of AMOS shell, the line numbers of error in the AMOS contextual log are for reference only.
- Due to limitation of AMOS shell, the script is only terminated with error on encountering the failure of MO write commands. For the failure of other commands such as COLI commands, the script is executed successfully and no error reported in AP. You need to check AMOS contextual log when debugging issue.

26.2.1.7 Task 'Initiate Import Configurations' is Failed (ERBS)

Prerequisites

You must have the following roles assigned to you:

- AutoProvisoning Operator
- Cmedit Administrator

Steps

1. Confirm the scenario:
   a. The Auto Provisioning node task status output indicates that `Initiate Import Configuration` task is failed, and the overall state is in integration suspended.
   b. Note any additional information in the `ap` node status output for the failing task.
2. If the job ID is provided, examine the output job verbose output:
   a. Open ENM CLI
   b. Examine the verbose output of the Job Id. Run the following command:

      ```
      cmedit import --status --job <Job_ID>  --verbose
      ```

   Note: It is recommended that in configuration files ManagedFunction Parent MO's are created in individual configuration files.
3. Update the configuration information using Bulk Configuration.

a. CM updates that are to be applied using the bulk cm files can be applied using the Bulk Configuration UI. For more information, see *Bulk Configuration UI Online Help*.

4. Remove the node Auto Provisioning data leaving the Network Element.

   a. Execute the following command to remove the Auto Provisioning node data and ignore the removal of the NetworkElement:

```
ap delete -i -n <nodename>
```

26.2.1.8 Task 'Activate Optional Features' is Failed (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

— Node Access

Steps

1. Confirm the scenario:

   a. Check the `Autointegration_report.log` from the node logs to verify the reason for Activate Optional Features failure.

      For more information on these logs, see Collect Node Logs for DU Radio Node (ERBS) on page 290.

   Note: This task failure does not prevent the Auto Provisioning application from continuing with the auto-integration procedure. Auto Provisioning reports the failure in the error logs and continue to the next task in the auto-integration procedure.

2. Manually execute the Activation of Optional Features.

   a. Operator must list all the optional features available on the node and execute the following command for each MO from ENM CLI.

```
cmedit  set MeContext=<nodeName>, ManagedElement=1, Sy →
stemFunctions=1, Licensing=1, OptionalFeatureLicense=< →
Optional Feature> featureState=ACTIVATED
```

26.2.1.9 Task 'Unlock Cells' is Failed (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

Steps

1. Confirm the scenario:
    a. The Auto Provisioning node task status output indicates that `Unlock Cells` is failed.
    b. Note the output of the task additional information.

    Note: Failure to `Unlock Cells` after node configuration does not prevent the Auto Provisioning application from continuing with the auto-integration procedure.

2. Manually unlock the cells using ENM CLI:
    a. Execute the following commands using ENM CLI for each node you want to unlock.

```
cmedit set MeContext=<nodeName>, ManagedElement=1, ENo →
deBFunction=1, EUtranCellFDD=<EUTranCellFDDId> adminis →
trativeState=UNLOCKED
```

26.2.1.10 Tasks 'Create CV or 'Upload CV' Failures (ERBS)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

Steps

1. Confirm the scenario:
    a. The Auto Provisioning node task status output indicates that `Create CV` or `Upload CV` task is failed.
    b. Note the output of the task additional information.

2. Identify the reason for failure:

a. If the additional information output indicates a backup failure and a report name, this report should be listed in the SHM Jobs page.

b. Select the failed job and view logs to identify the reason for the failure.

3. Manually create and upload a backup using the SHM (Software and Hardware Manager) application.

    a. Using SHM select the node that was integrated and follow the SHM online help description to manually create a node backup and upload it to ENM.

26.2.1.11 Tasks 'Create Backup' or 'Upload Backup' Failures

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output indicates that `Create Backup` or `Upload Backup` task is failed.

    b. Note the output of the task additional information.

    Note: Failure to create or upload a backup after node configuration does not prevent the Auto Provisioning application from continuing with the auto-integration procedure.

2. Identify the reason for failure:

    a. If the additional information output indicates a backup failure and a report name, this report should be listed in the SHM Jobs page.

    b. Select the failed job and view logs to identify the reason for the failure.

3. Manually create and upload a backup using the SHM (Software and Hardware Manager) application.

    a. Using SHM select the node that was integrated and follow the SHM online help description to manually create a node backup and upload it to ENM.

26.2.1.12 Task 'Node Synchronization Notification' Remains at Waiting

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output indicates that the `Node Synchronization Notification` task is Waiting.

2. Check the node sync status:

    a. It is possible that the node is still synchronizing. To check the current synchronization state of the node, use the following command:

    ```
    cmedit get <nodeName> CmFunction.syncStatus
    ```

    If the `syncStatus` of the node is in any of the following states, synchronization is still in progress:

    — PENDING

    — DELTA

    — TOPOLOGY

    — ATTRIBUTE

    If the syncStatus is `UNSYNCHRONIZED`, it is possible that the node failed to synchronize (failure reason maybe available in error log). To start a manual re-sync, you need to reset the node supervision, using the following commands:

    ```
    cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision= 1
    active= false
    cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision= 1
    active= true
    ```

    b. If the resynchronization is successful, the task 'Node Synchronization Notification' progresses to 'Received'.

    c. If the resynchronization fails, see CM Node Synchronization Troubleshooting - CPP Based Nodes on page 47 .

3. Check if Node Synchronization failed due to a model mismatch

The synchronization failure could be caused by a problem with the `ossModelIdentity` (OMI) attribute value assigned in the NetworkElement MO. To verify this check the CPP error log (see CM Node Synchronization Troubleshooting - CPP Based Nodes on page 47) for synchronization errors, of the following type: "Could not synchronize network element *<nodeName>* as its version is not supported by ENM." In this case, the `NetworkElement::ossModelIdentity`It is possible that the node is still synchronizing. To check the current synchronization state attribute needs to be set, to inform ENM what version to treat the node as.

a. Run the following command from the ENM CLI to identify a supported OMI:

```
cmedit describe -ne <nodeType>
```

b. Run the following command to set the OMI:

```
cmedit set NetworkElement=<nodeName> ossModelIdentity=xx-xx-xx
```

26.2.1.13 Task 'Ready For Service Notification' is Failed (MSRBS_v1)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Node Access

Steps

1. Confirm the scenario:
    a. The Auto Provisioning node task status output indicates that `Ready For Service Notification` is failed.
2. Check the node logs for errors.
    a. Check the Auto-integration.log to see if there were any messages indicating why `Ready for service Notification` failed.

    For more information on these logs, see Collect Node Logs on page 290

26.2.1.14 Task 'Validate Configuration' Unable to Validate NETCONF Files (Radio Node)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output indicates that the `Validate Configuration` task is failed.

    b. Note any additional information in the `ap` node status output for the failing task.

    c. Verify that the additional information is describing errors in a file inputted in the NETCONF format.

2. Verify the configuration files against the node Managed Object Model:

    a. Based on the Additional Information, compare the content of the inputted configuration files and the Managed Object Model for the specific UP (Upgrade Package) that is being used to integrate the node.

    b. Update the configuration files to remove any invalid inputs.

3. Identify the reason for the NETCONF failure:

    a. During the `Validate Configuration` task, AP delegates validation of NETCONF files to the Node Plugins service group. On rare occasions there may be reasons where an operator may want to skip the NETCONF validation.

    This may occur if:

    — You are unable to execute remote validation due to unavailability of external node plugin.

    — Model is introduced with non-backwards compatible changes through Release Independence, which is unsupported by Node Plugin Validation for Radio Node.

    To check if the problem lies in the unavailability of the external plugin service, check the Log Viewer and search for errors within the 'nodeplugins' service group.

    Additional information for the failure reason is also captured in the Auto Provisioning logs.

4. Skip NETCONF validation:

    a. In this case, unavailability of the Node Plugin or an unsupported model it is a non-recoverable error in the Auto Provisioning

application. This results in failure to auto-integrate the node. If required, NETCONF file validation can be skipped by executing the following command from the ENM CLI.

```
ap order -nv file:<fileName>
```

26.2.1.15 Upload Fixed Site Basic and Wait for Next Run of Integration

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. Confirm the scenario:
    a. The Auto Provisioning status output shows the task `Node Installing Configurations` in failed and the Additional Information shows that the `SiteBasic` file has NETCONF errors.
2. Download and fix the `SiteBasic` file.
    a. From ENM CLI execute the following command:

    ```
    ap download -i -n <nodename>
    ```

    b. Fix the issue with the `SiteBasic` file.
3. Upload a new `SiteBasic` file:
    a. Using AutoProvisioning Upload drag and drop the updated `SiteBasic` file to the ENM CLI (or use the Upload button on the UI) and execute the following command:

    ```
    ap upload -n <nodename> file:SiteBasic.xml
    ```

4. Wait for the next integration for the node to fetch the updated `SiteBasic` file.

26.2.1.16 Fix Configuration Files

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. Confirm the scenario:

    a. Check that the Auto Provisioning status output shows the task `Node Downloading Configurations` in failed.

    b. Check the Auto Provisioning Status Additional Information.

2. Ensure that the configuration files are generated and stored in SMRS. For more information, see Collect the Integration Artifacts and Integration Project File on page 290. In case the configuration files are deleted from SMRS, reorder the node with Auto Provisioning.

3. For LMT integration, in the `SiteInstallation` file ensure that the path to the `RbsSummary` file is correct.

4. Rectify any errors and rerun the order with the updated project zip.

26.2.1.17 Upgrade Package Deleted in SHM

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. Confirm the scenario:

    a. Check that the Auto Provisioning status output shows the task `Node Downloading Configurations` in failed and the Additional Information indicates that the upgrade package is not available.

2. In SHM check that the Upgrade Package referred to in the `NodeInfo` file still exists. If Upgrade Package has been deleted it will need to be re-imported to SHM.

26.2.1.18 Rectify AIWS Port Configurations

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. AIWS port is not open, refer to the [31] ENM NIG Connection Matrix.

26.2.1.19 Configure Software Management Task Fails to Update SwM MO

Prerequisites

You must have the following roles assigned to you:

— Cmedit_Administrator

— SECURITY_ADMIN

— Scripting_Operator

Steps

1. Confirm the scenario:
    a. The Auto Provisioning node status output indicates that the `Configure Software Management` task has failed.
        i. Note the output of the task additional information.
    b. In **User Management**, create a user with sufficient privileges to access the SMRS.
        i. Launch **User Management**.
        ii. Create a user with role as `FIELD_TECHNICIAN`.
        iii. Note the username and password
    c. Get SMRS IP address.
        i. Log on to the Shell Terminal on Scripting.
        ii. Retrieve the SMRS IP address:

```
[<username>@scp-1-scripting(enmHost) ~]$ cat /ericsson/tor/data
/global.properties  |
grep svc_CM_vip_ipaddress

svc_CM_vip_ipaddress=<ipaddress>
```

d. Log on to the ENM and set the newly created user information to SwM MO.

i. On the ENM CLI, execute the following command:

```
cmedit set <nodeFDN>,SystemFunctions=1,SwM=1 defaultUri="sftp:/
/<newly_created_user>@<smrs_ip><upgrade_package_path>", default
Password={password=<newly_created_user_password>, cleartext=tru
e}
```

Example

```
cmedit set SubNetwork=AP_1924058,ManagedElement=LTE01dg2ERBS00018,S
ystemFunctions=1,SwM=1 defaultUri="sftp://hsi_user@192.168.0.186/sm
rsroot/software/msrbs_v1/RadioNode_R4D25_release_upgrade_package",
defaultPassword={password=H5!PA55w0rd, cleartext=true}
```

Note: The upgrade package is located at `/smrsroot/software/<node_type>/<upgrade_package_name>`.

26.2.2 Automatic Hardware Replace Troubleshooting Steps

> This section describes the steps to resolve the issues that may arise during the execution of hardware replace.

26.2.2.1 Hardware Replace 'Node Up Notification' Remains at Waiting (MSRBS_v1)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Node Access

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output `Node Up Notification` task is Waiting.

2. Collect the `Autointegration_report.log`.

For more information about how to retrieve this log, see Collect Node Logs on page 290.

3. Ensure that the hardware serial number in the replace command matches the hardware serial number of the node.

    a. Confirm the hardware serial number of the node in the `Autointegration_report.log` in the node log. By finding an entry as below, ensure that the node hardware serial number is the same as that of the replaced node in ENM, visible using the `ap` view.

    ```
    2010/01/01 00:02:36 [VLAN 2904:20%] Subject of vendor certificate:
    /C=SE/O=Ericsson/CN=<hardwareSerialNumber>.ericsson.com for ICF dow
    nload
    ```

    An error due to mismatched hardware serial number will result in the following entry being shown in the node log, each time the node attempts to fetch the configuration file.

    ```
    2010/01/01 00:08:27 [VLAN 2904:20%] ICF fetching from AIWS: 131.160
    .146.81 failed
    2010/01/01 00:08:27 [VLAN 2904:20%] Connected to AIWS but file not
    found
    ```

    If the hardware serial number is incorrect, the operator must delete the node from ENM using `ap` delete and rerun the replace command with the correct hardware serial number.

4. Check if the node up message is sent successfully.

    a. Verify that the `Autointegration_report.log` from node logs contains a message to confirm that the node up message is sent successfully. For more information, see Collect Node Logs on page 290.

    ```
    2017/07/07 05:35:02 [80%] Ready to continue OSS synchronization.
    2017/07/07 05:35:02 [80%] Notifying OSS to start communication.
    2017/07/07 05:35:02 [80%] Node discovery trap parameters: O&M IP ad
    dress:<ipAddress> Node ID: SubNetwork=<subNetworkName>,SubNetwork=<
    subNetworkName>,MeContext=<nodeName>,ManagedElement=<nodeName>
    ```

    If the node up message was not sent by the node then node support is required to investigate the fault. If the node up was sent by the node but not received by ENM then you must collect logs. For more information, see Collect Node Logs on page 290.

26.2.2.2 Hardware Replace 'Node Synchronization Notification' Remains at Waiting (MSRBS_v1)

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

— Node Access

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output indicates that the `Node Synchronization Notification` task is Waiting.

2. Check the node sync status:

    a. It is possible that the node is still synchronizing. Current synchronization state of the node may be visible in the additional information and can also be obtained using the following command::

    ```
    cmedit get <nodeName> CmFunction.syncStatus
    ```

    If the `syncStatus` of the node is in any of the following states, synchronization is still in progress:

    — PENDING

    — DELTA

    — TOPOLOGY

    — ATTRIBUTE

    If the syncStatus is `UNSYNCHRONIZED`, it is possible that the node failed to synchronize (failure reason maybe available in error log). To start a manual re-sync, you need to reset the node supervision, using the following commands:

    ```
    cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision= 1
    active= false
    cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision= 1
    active= true
    ```

    b. If the resynchronization is successful, the task `Node Synchronization Notification` progresses to 'Received'.

    c. If the resynchronization fails, see CM Node Synchronization Troubleshooting - Nodes Supporting ECIM on page 13 .

3. Check if Node Synchronization failed due to a model mismatch

The synchronization failure could be caused by a problem with the `ossModelIdentity` (OMI) attribute value assigned in the NetworkElement MO. To verify this check the error log (see Unsupported Node Version COM/ECIM (Treat-As Functionality) on page 28) for synchronization errors, of the following type: "Could not synchronize the node *<nodeName>* as its version is not supported by ENM." In this case, the `NetworkElement::ossModelIdentity` needs to set, to inform ENM what version to treat the node as.

a. Run the following command from the ENM CLI to identify a supported OMI:

```
cmedit describe -ne <nodeType>
```

b. Run the following command to set the OMI:

```
cmedit set NetworkElement=<nodeName> ossModelIdentity=xx-xx-xx
```

c. Initiate the node synchronization again using the following command:

```
cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision=1 a →
ctive=false
cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervision=1 a →
ctive=true
```

26.2.2.3 Hardware Replace 'Configure DHCP' or 'Remove DHCP Client Configuration' is Failed

Prerequisites

You must have the following roles assigned to you:

— DHCP_Administrator

Steps

1. Confirm the scenario:

   a. The Auto Provisioning node task status output `Configure DHCP` task is Failed.

   b. Note the Additional Information column of the `Configure DHCP` task to know the failure reason.

      Configure DHCP has failed for the following reasons:

Table 14 Configure DHCP Faiure Reasons

Additional Information	Description
Client identifier is not unique	Hardware serial number is used as a Client identifier. Check if the hardware serial number is correct. Update DHCP configuration by `dhcp client` commands if necessary.
Client IP is not unique	Fixed IP address is used as Client IP. Check if fixed IP address is correct. Update DHCP configuration by `dhcp client` commands if necessary.
Hostname is not unique	Node name is used as hostname. Check if DHCP configuration exists. Update DHCP configuration by `dhcp client` commands if necessary.
Validation of IP address: <ipAddress> failed. Address is outside network: <subnet> with mask: <netmask>.	Initial IP address is used as Client IP. Check if initial IP address conflicts with DHCP configuration. Update DHCP configuration by `dhcp network` and `dhcp client` commands if necessary.

c. Use the following commands to view, add, or delete DHCP configuration:

```
dhcp network add -s <subnet> -n <netmask>
dhcp network delete -s <subnet>
dhcp client view <serialNumber>
dhcp client view -h <nodeName>
dhcp client view -i <fixedIPAddress>
dhcp client add <serialNumber> -h <nodeName> -i <fixedIPAddress> -s
 <subnet>
dhcp client delete <serialNumber>
```

Note: For more information, see ENM *CLI Online Help*.

2. In the event of Remove DHCP verify the Additional Information output of the AutoProvisioning status.

   a. If the failure reason is `Client configuration not found`, this error can be ignored. Otherwise, attempt to remove DHCP client configuration manually:

```
dhcp client delete <serialNumber>
```

Verify DHCP messages to confirm that DHCP configuration succeeded. For more information, see Collect DHCP Logs on page 293.

26.2.2.4 Generate Security Fails due to Unsupported Configuration

Prerequisites

You must have the following roles assigned to you:

— Cmedit_Operator

— AutoProvisioning_Operator

Steps

1. Confirm the scenario:
    a. The Auto Provisioning node task status output Generate Security task is Failed and the Additional Information shows `Error generating ossNodeProtocol file for node <nodename>. Check Node Certificates are successfully enrolled`.
2. Check if the hardware replace is updating node security parameters.
    a. Execute the following command through ENM CLI:

    ```
    ap view -n <nodename>
    ```

    b. Verify that the `SubjectAltName` value is populated.
3. Verify the node configuration is suitable for execution of Hardware replace.
    a. Execute the following command to retreive the node FDN through ENM CLI:

    ```
    cmedit get <NodeName> Ikev2PolicyProfile
    ```

    b. Output the `Ikev2PolicyProfile` attributes using the FDN that was returned from the above command

    For example: **`cmedit get ManagedElement=<NodeName>,Transport=1,Ikev2PolicyProfile=<Ikev2PolicyProfileName>`**

    c. Verify that the `Ikev2PolicyProfile` contains a credential attribute referencing an `ipsec nodecredential` MO.

    For example:
    `credential="ManagedElement=1,SystemFunctions=1,SecM=1,CertM=1,NodeCredential=ipsecNodeCredential`

d. If mulitple `Ikev2PolicyProfile` MO exist they must all be referencing the same NodeCredential.

e. Verify that the referenced `ipsecNodeCredential` MO contains the following attributes and their values are populated:

   — `enrollmentServerGroup`

   — `keyInfo`

   — `renewalMode`

   — `enrollmentAuthority`

   — `subjectName`

Results

If any of the above are not populated the configuration is unsupported for hardware replace with updated ipsec parameters, consult node documentation to verify node configuration. Alternatively, for non-ipsec configuration hardware replace re-execute the use-case without the `subjectAltName` included as part of the AutoProvisioning Hardware replace `nodeInfo.xml`.

26.2.3 Automatic Expansion Troubleshooting Steps

> This section describes the steps to resolve the issues that may arise during the execution of node expansion.

26.2.3.1 Expansion Notification Task Remains at Waiting Status

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— LogViewer Operator

Steps

1. Confirm the scenario:

   a. The Auto Provisioning node task status **Expansion Notification** task is stuck at waiting.

2. Check the **Additional Information** column of the **Expansion Notification** task. The column displays one of the following texts.

Option	Description

Technician Present	If the **Additional Information** is **Technician Present**, node waits up until the **second legal maintenance** button is pressed to resume the workflow:
	a. Confirm the value of `TechnicianPresent MO` attribute in ENM CLI to **PRESENT**.
	`# cmedit get <nodeName> OnSiteActivities.technicianPresent`
	b. Field Technician confirms if the `Maintenance` LED status is steady blue or not.
	• If the `Maintenance` LED light is unsteady blue, wait until it becomes steady blue.
	• If the `Maintenance` LED light is steady blue, the following actions can resume the expansion workflow:
	i. Field Technician waits for 30 seconds, then presses the **maintenance** button on the baseband node (less than 7 seconds) again to resume the expansion workflow and waits for `Maintenance` LED light to be off.
	ii. Alternatively, resume the expansion workflow directly by running the AP command.
	`# ap resume -n <nodeName>`
	After the AP command is run, the Field Technician must press **maintenance** button on the baseband node (less than 7 seconds) again and wait for `Maintenance` LED light to be off.

Waiting for notification or resume/ cancel operation	If the **Additional Information** is **Waiting for notification or resume/cancel operation**, node expansion workflow fails because an invalid **maintenance** button is pressed on the baseband node. a. Confirm the value of `TechnicianPresent MO` attribute in ENM CLI to **NOT_PRESENT**. `# cmedit get <nodeName> OnSiteActivities.technicianPresent` b. Field Technician confirms the `Maintenance` LED light is off.

Option	Description
	c. The following options can resume the expansion workflow: • Valid **maintenance** button is pressed on a baseband node. — Field Technician presses **maintenance** button on a baseband node (greater than 2 seconds and less than 7 seconds) and waits for the node to enter full maintenance mode (`Maintenance` LED light steady blue). — Field Technician presses **maintenance** button on baseband node (less than 7 seconds) again after an interval of greater than 30 seconds to resume the expansion workflow and waits for the node to quit maintenance mode (`Maintenance` LED light off). • Alternatively, the ENM Operator can resume the expansion workflow directly by running the AP command without entering full maintenance mode. `# ap resume -n <nodeName`

26.2.3.2 Expansion Task 'Import Configurations' is Failed

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

Steps

1. Confirm the scenario:
   a. The Auto Provisioning node task status output indicates that Import Configuration task is failed, and the overall state is in expansion suspended.
   b. Note any additional information in the ap node status output for the failing task.
2. Fix the file that has the reported issues and retry.

a. For BULK CM file, the job ID is provided. Examine the output job verbose output:

   i. Open ENM CLI.

   ii. Run the following command:

   ```
   cmedit import --status --job <Job_ID>  --verbose
   ```

   iii. Examine the verbose output of the Job ID.

   iv. If the reason for the import failure can be identified from the verbose import job status output, you can update the file that is causing the issue.

b. For NETCONF file, the job ID is not provided. Examine the ap node status output:

   i. Check the Message ID in the error messages of additional information, find the corresponding edit-config rpc in the file. If the Message ID is in the format of `message-id is unknown, the rpc edit-config message sequence is #<sequence>`, count the edit-config rpc in the file and locate the failed rpc according to the sequence.

   ii. If the reason for the import failure can be identified from additional information in the ap node status output, you can update the file that is causing the issue.

c. For amos file, the job ID is not provided. Examine the ap node status output:

   i. Click the `<contextual link>` in additional information then check AMOS contextual log for details.

   ii. If the reason for the import failure can be identified from additional information in the ap node status output, you can update the file that is causing the issue.

   Note:
   - Due to limitation of AMOS shell, the line numbers of error in the AMOS contextual log are for reference only.
   - Due to limitation of AMOS shell, the script is only terminated with error on encountering the failure of MO write commands. For the failure of other commands such as COLI commands, the script is executed successfully and no error reported in AP. You need to check AMOS contextual log when debugging issue.

26.2.3.3 Restore Backup Task Remains at Started

> The **Restore Backup** task stuck in `Started` status for 60 minutes or longer and the reason in **additional info** indicates `timeout`.

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Cmedit Administrator

Steps

1. Check the **Additional Information** column of the **Restore Backup** task displays `Backup Name: <backupname>. Restore failed: timeout`.
2. Check the `progressReport` attribute of the `BrmBackup MO` filtered with *<backupname>* in ENM CLI.

   Example

   ```
   cmedit get <nodeName> BrmBackup.backupName==<backupname> BrmBa →
   ckup.progressReport
   ```

   Result: Check the value of `actionName` and `result` attribute. If restore backup is successful, then go to step 4. If restore backup has failed, create the **`Restore Job`** manually if needed.
3. Check whether there is a Node Synchronization issue.

   There can be an instance when the node is still synchronizing. To check the current synchronization state of the node, run the following command:

   ```
   # cmedit get <nodeName> CmFunction.syncStatus
   ```
4. syncStatus can have the following status:

   — If the status is PENDING, DELTA, TOPOLOGY, or ATTRIBUTE, synchronization is still in progress.

   — If the status is UNSYNCHRONIZED, the node failed to synchronize.

   Note: Failure reason may be available in error log.
5. Reset the node supervision to start a manual re-sync, by running the following commands:

```
# cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervis →
ion=1 active=false
# cmedit set NetworkElement=<nodeName>,CmNodeHeartbeatSupervis →
ion=1 active=true
```

Result: If the resynchronization is successful, repeat step 3 to check restore result again.

26.2.4 General AP Troubleshooting Steps

> This section describes the steps to resolve the general issues that may arise during the execution of auto provisioning activities.

26.2.4.1 Task 'Cancel Security' Fails

Prerequisites

You must have the following roles assigned to you:

— AutoProvisoning Operator

— Log Viewer Operator

Steps

1. Confirm the scenario:

    a. The Auto Provisioning node task status output `Cancel Security` task is failed and has the text **MeContext/NetworkElement in node FDN [NetworkElement=<nodeName>] , but no normalized node reference**.

    ```
    ap status -n <nodeName>
    ```

2. Check to see if the NetworkElement exists on the system, and is SYNCHRONIZED:

    ```
    cmedit get NetworkElement=<nodeName>
    cmedit get <nodeName> CmFunction.syncStatus
    ```

3. If the NetworkElement exists and is SYNCHRONIZED, check to see if the ManagedElement also exists on the system:

    ```
    cmedit get <nodeName> ManagedElement
    ```

If the ManagedElement does exist:

a. Manually delete the NetworkElement and ManagedElement data:

```
cmedit set <nodeName> CmNodeHeartbeatSupervision active=false
cmedit action <nodeName> CmFunction deleteNrmDataFromEnm
cmedit delete <nodeName> NetworkElement -ALL
```

b. Attempt the delete of the node autoprovisioning data again:

```
ap delete -n <nodeName>
```

If the ManagedElement does not exist:

a. Unsynchronize the NetworkElement:

```
cmedit set <nodeName> CmNodeHeartbeatSupervision active=false
```

b. Attempt the delete again:

```
ap delete -n <nodeName>
```

4. If the NetworkElement is not SYNCHRONIZED:

   a. Delete the NetworkElement:

   ```
   cmedit delete <nodeName> NetworkElement -ALL
   ```

   b. Attempt the delete again:

   ```
   ap delete -n <nodeName>
   ```

5. If the NetworkElement does not exist, attempt to delete again using the `cmedit` command.

   — Delete AP project.

   ```
   cmedit delete Project=<projectName> -ALL
   ```

26.2.4.2 Email with Node Status Fails to Deliver

> Email with node status fails to be delivered.

Prerequisites

You must have the following role assigned to you:

— AutoProvisoning Operator

Steps

1. Check the current expansion node status with AP command.

   ```
   # ap status -n <nodeName>
   ```

2. Check whether there is an incorrect or no email address configured in the project zip file.
   - If there is an incorrect or no email address configured, correct or fill in the email address.
   - If there is correct email address configured, go to step 3.
3. Check whether there is a problem on the outbound email configuration on ENM site.
   - Check information on the outbound email configuration. Refer to *Fault Management Email Alarm Routing functionality* in ENM Monitoring System Administrator Guide - [Reference 26] .
   - The failure reason is captured in the Auto Provisioning logs. For more information on gathering these logs, see Collect ENM Logs.

26.2.4.3 Task 'Generate Security' Fails

> Generation of Security can fail for an MSRBS_V1 node, if the serial number being used was previously used during integration of a node with a different node name. To resolve this, the Public Key Infrastructure End Entity needs to be deleted before the node can be reintegrated. The following troubleshooting steps outline how to diagnose and resolve this issue.

Prerequisites

Requires a user with the following roles:

- AutoProvisoning Operator
- Log Viewer Operator

Steps

1. Confirm the scenario in AP GUI:

   The Auto Provisioning node task status output 'Generate Security' task is 'Failed' with Additional Information: 'Security Service Error'.

2. Confirm the scenario in LogViewer:

   The following error message must exist in LogViewer:

```
[Check EndEntity failed] [ERROR: Exception : class [com.erics
son.nms.security.nscs.cpp.service.CppSecurityServiceException
] : msg [Error while creating entity: _<Node Name>_-oam. Subj
ect already used for entity: _<Node Name>_-oam] while getting
 enrollment info]
```

3. Delete the AP node:

```
> ap delete -n <Node Name>
```

4. Delete Public Key Infrastructure End Entity:

   Refer Permanent Deletion of EndEntites

26.3 Data Collection for Auto Provisioning

> This section outlines the files and logs required to troubleshoot the issues that may arise when executing AutoProvisioning activities.

Depending upon the use-case, troubleshooting scenario, ENM deployment, and node type different logs and files are required for troubleshooting.

The following files are required:

— The pre-created project and the files described in the Collect the Integration Artifacts and Integration Project File on page 290 (for node integration and hardware replace).For expansion and reconfiguration only project file is required.

— DDP information for the deployment.

— A screen shot or export of the auto provisioning node status output of when the issue has occurred.

— Node logs (for node integration and hardware replace).

If DDP is not available, follow Retrieve Auto Provisioning Service Group Logs on page 288 and Retrieve External Service Group Logs on page 289.

Once you have the logs, follow the steps outlined in Attach All Logs or Node Files to a Customer Support Request on page 294.

26.3.1 Collect ENM Logs

This section describes the procedure to collect ENM logs.

26.3.1.1 Retrieve Auto Provisioning Service Group Logs

If DDP is available this step is not required for most issues.

Prerequisites

To retrieve ENM logs you must have access to connect to Virtual Machine. For more information, see Connect to a Virtual Machine on page 2.

Steps

1. Connect to the `apserv` and `msap` Virtual Machines (VMs).

   Follow the instructions below to connect to a virtual machine and log on to the `apserv` and `msap` VMs on all service cluster nodes.

2. Collect the ENM logs.

   a. Copy the logs from each svc-* (or Service Groups only) to the directory `/ericsson/tor/data/` on the Management Server. These logs will later be attached to the CSR.

   ```
   # Syntax: cp /ericsson/3pp/jboss/standalone/log/server.log /ericsso →
   n/tor/data/<service_group>-server.log # Example: cp /ericsson/3pp/j →
   boss/standalone/log/server.log /ericsson/tor/data/svc-1-apserv-serv →
   er.log
   ```

   Certain scenarios may require lower level debug logs. For more information about how to retrieve these logs, see Retrieve Auto Provisioning Service Group debug logging.

26.3.1.2 Retrieve Auto Provisioning Service Group Debug Logging

Prerequisites

To retrieve ENM logs you must have access to connect to Virtual Machine. For more information, see Connect to a Virtual Machine on page 2.

Steps

1. Connect to the `apserv` and `msap` Virtual Machines (VMs).

   Follow the instructions below to connect to a virtual machine and log on to the `apserv` and `msap` VMs on all service cluster nodes.

2. Change the JBoss containers logging level to DEBUG.

    a. For each VM run the following command.

    ```
    /ericsson/3pp/jboss/bin/jboss-cli.sh -c "/subsystem=logging/logger=
    com.ericsson.oss:change-log-level(level=DEBUG)"
    ```

    Note: Enabling logging on applications can have an adverse effect on the performance of the application.

3. Re-run the scenario with the fault. DEBUG level logs will now be generated.

4. Change the JBoss containers logging level back to INFO.

    a. For each VM run the following command.

    ```
    /ericsson/3pp/jboss/bin/jboss-cli.sh -c "/subsystem=logging/logger=
    com.ericsson.oss:change-log-level(level=INFO)"
    ```

    AP has external dependencies. If required, collect logs from the following and attach to the CSR:

    Note: Enabling logging on applications can have an adverse effect on the performance of the application.

26.3.1.3 Retrieve External Service Group Logs

> Auto Provisioning interacts with different ENM service groups. Dependent on the use-case and issues that arise logging from additional service groups.

If DDP is available this step is not required for most issues.

Prerequisites

To retrieve ENM logs you must have access to connect to Virtual Machine. For more information, see Connect to a Virtual Machine on page 2.

Steps

1. Connect to the `<external service group>` Virtual Machines (VMs).

    Follow the instructions below to connect to a virtual machine and log on to the `apserv` and `msap` VMs on all service cluster nodes.

2. Collect the ENM logs.

a. Copy the logs from each svc-* (or Service Groups only) to the directory `/ericsson/tor/data/` on the Management Server. These logs will later be attached to the CSR.

```
# Syntax: cp /ericsson/3pp/jboss/standalone/log/server.log /ericsso
n/tor/data/<service_group>-server.log # Example: cp /ericsson/3pp/j
boss/standalone/log/server.log /ericsson/tor/data/svc-1-apserv-serv
er.log
```

26.3.2 Collect the Integration Artifacts and Integration Project File

Prerequisites

To retrieve ENM logs you must have access to connect to a virtual machine. For more information, see Connect to a Virtual Machine on page 2.

Steps

1. Collect the generated node integration files.

   a. The files are located per node in the following shared directory and can be accessed from any of the service groups

   ```
   /ericsson/tor/smrs/smrsroot/ai/<Node Type>/<Node Name>
   ```

2. Collect the node artifact files

   From the ENM CLI, run the following commands to download all required artifacts for that node.

   a. To download all initial artifacts:

   ```
   ap download -i -n <nodeName>
   ```

   b. To download all `Ordered` artifacts:

   ```
   ap download -o -n <nodeName>
   ```

3. The files and project zip file used to order the node integration must be attached to the CSR.

26.3.3 Collect Node Logs

26.3.3.1 Collect Node Logs for DU Radio Node (ERBS)

The following node logs exist:

Log File	Description	Path	Available
`autointegrationconfigurationReport.log`	Configuration Report in respect of the current Integration.	`/c/logfiles/`	At any stage during the Integration.
`Autointegration_report.log`	This contains traces (`se.ericsson.lte.rbs.omf.mao.rbsconfiguration`) collected in respect of the current Integration.	`/c/logfiles/autointegration/`	At any stage during the Integration.
`autointegration/autointegration_logs_<nodeName>.zip`	This contains all the Auto Integration logs in respect of the most recent Integration.	`c/logfiles/autointegration/`	When Integration is Complete or Canceled.

For more information, see *Node Data Collection Guidelines*.

26.3.3.2 Collect Node Logs for Baseband Radio Node

The following node logs exist:

Log File	Description	MO Class	<log_MO_FDN>	Available
AiLog	Logs all AutoIntegration events.	Log	SubNetwork=*<subNetworkName>*,ManagedElement=*<nodeName>*,SystemFunctions=1,LogM=1,Log=AiLog	After the OAM connection is up.

For more information, see *Node Data Collection Guidelines*.

26.3.3.3 Collect Node Logs for MSRBS_V1

The following node logs exist:

Log File	Description	File Path
`Auto-integration log`	Log contains information about auto integration activities and status.	`/oss/permanent/`

For more information, see *Node Data Collection Guidelines*.

26.3.3.4 Collect Node Logs for Router 6000 Node (Router 6672, Router 6675, and Router 6x71)

The following node logs exist:

Log File	Description	Available	Collect Method (On Node)
`system log`	AUTOD system log	At any status during the integration	CLI: `show log persistent | grep AUTOD` CLI: `show log | grep AUTOD`
`/var/log/ai_apply_netconf.log`	Log for AI applying NetConf messages in `OssNodeProtocol.xml`	When node AI status is: Configuration from `SiteBasic` File applied	CLI: `more /var/log/ai_apply_netconf.log`
`/var/log/ai_capture_engineid.log`	Log for AI automatically capturing SNMP engine ID	When node AI status is: NetConf messages in `OssNodeProtocol` file applied	CLI: `more /var/log/ai_capture_engineid.log`
`/var/log/ai_failed_netconf_msg.xml`	Error log for AI applying NetConf messages in `OssNodeProtocol.xml`	When node AI status is: Failed to apply netconf messages in `OssNodeProtocol` file.	CLI: `more /var/log/ai_failed_netconf_msg.xml`
`/var/log/ai_failed_configif.log`	Error log for AI automatically configuring interface for DHCP (one case of errors)	When node AI status is: Failed to contact DHCP server, no valid DHCP offer received	CLI: `more /var/log/ai_failed_configif.log`

Log File	Description	Available	Collect Method (On Node)
`/var/log/ai_failed_unconfigif.log`	Error log for AI automatically unconfiguring interface for DHCP	When node AI status is: Internal error: failed to unconfigure interface	CLI: `more /var/log/ai_failed_unconfigif.log`
`/var/log/ai_failed_configmgmt.log`	Error log for AI configuring management interface when initialization (one case of errors)	When node AI status is: Internal error: failed to initialize auto-integration	CLI: `more /var/log/ai_failed_configmgmt.log`
`/var/log/ai_failed_configsnmpreceiver_step1.log`	Error log for AI configuring SNMP receiver before capturing SNMP engine ID	When node AI status is: Failed to configure SNMP receiver	CLI: `more /var/log/ai_failed_configsnmpreceiver_step1.log`
`/var/log/ai_failed_configsnmpreceiver_step2.log`	Error log for AI configuring SNMP receiver after capturing SNMP engine ID	When node AI status is: Failed to send SNMP trap and detect synchronization	CLI: `more /var/log/ai_failed_configsnmpreceiver_step2.log`

For more information, see *Node Data Collection Guidelines*.

26.3.4 Collect DHCP Logs

> When executing Zero Touch node integration or hardware replace, networking issues may arise when the node is trying to retrieve configuration information from ENM's DHCP. The below section outlines the steps required to see additional DHCP logging.

1. Log on to the ENM Command Line Interface with either of the following roles:
   - DHCP_Administrator
   - DHCP_Service_Operator
   - DHCP_Monitor user role

Refer to section *Role Based Access Control (RBAC) Management* in the ENM System Administrators Guide for details.

2. Run the following command to start DHCP monitor session:

```
# dhcp monitor start
```

3. Run the following command to stop DHCP monitor session:

```
# dhcp monitor stop
```

4. Run the following command to display DHCP monitor session:

```
# dhcp monitor view
```

Refer to *CLI Online Help* for details.

26.3.5 Attach All Logs or Node Files to a Customer Support Request

Complete the task following the instructions:

Steps

1. Execute the `/opt/ericsson/enminst/bin/enm_version.sh` and store the output in the `/enm/enm_error/` directory to ensure it gets included in the `report.tar` file.

   If the directory `/enm/enm_error/` does not exist, create it using the command:

```
mkdir -p /enm/enm_error
```

2. Store the output in `/enm/enm_error` run the following command:

```
/opt/ericsson/enminst/bin/enm_version.sh > /enm/enm_error/enm_ver.out
```

3. Collate the collected files using the following command:

```
# tar cvf report.tar  /enm/enm_error/
```

4. Zip up the report for attachment to the Customer Support Request using the following command:

```
# gzip report.tar
```

   Write a reproduction scenario (step by step how to reproduce the problem) to include in the Customer Support Request.

5. Clean up the directory using the following command:

```
# rm -rf  /enm/enm_error/
```

26.4 Auto Provisioning Housekeeping

> This section outlines the Auto Provisioning Housekeeping activity and issues that may arise when it is executed.

26.4.1 Projects Housekeeping

If a node reaches an integrated or canceled state in Auto Provisioning (AP), then AP housekeeping cleans old data after seven days. AP housekeeping can also delete projects if the last node in a project is deleted and there are no profiles associated with that project.

To verify the scenario, follow Collect ENM Logs on page 288. Search the logs for entries related to logging the delete activity with the node name. If the node is deleted by the user **autoprovisioning_application_system**, then AP Housekeeping cleaned up the node.

To view the historic task output for the deleted node, use the search criteria field in the log viewer application, which filters the node task output.

```
host:"*apserv" AND message:AUTO_PROVISIONING.TASK_OUTPUT AND message:"NODE\=<Nod
eName>"
```

If the deleted node is in a completed end state, then the network element can be seen using the command.

```
cmedit get NetworkElement=<NodeName>
```

26.4.2 SNMP Users Housekeeping

As part of securing SNMP communication channels between ENM and a node, `snmpusers` need to be generated using data stored in a secure admin parameter location. These users need to be automatically removed when they are no longer needed. AP automatically executes an audit to remove these at 02:30 AM every day.

Reference List

[1] *ENM System Administrator Guide*, 1/1543-AOM 901 151

[2] *ENM Network Integration Guideline*, 1/102 72-AOM 901 151.

[3] *ENM Operator's Guide*, 1/1553-AOM 901 151

[4] *ENM Security System Administrator Guide*, 2/1543-AOM 901 151

[5] *VNF-LCM Installation Instructions*, 1/1531-CNA 403 3313, available in the ENM Installation and Support CPI Library.

[6] *Typographic Conventions*, 3/1551-FCK 101 05

[7] *ENM Backup and Restore System Administrator Guide*, 3/1543-AOM 901 151

[8] *ENM Configuration System Administrator Guide*, 1/1543-AOM 901 151-1

[9] *ENM Data Collection Guideline*, available from local Ericsson Support.

[10] *ENM Interwork Description for File Lookup Service (FLS)*, 1/155 19-CNA4033301

[11] *ENM Performance Management System Administrator Guide*, 1/1543-AOM 901 151-3

[12] *ENM Installation Instructions*, Available from local Ericsson Support

[13] *Manage Security User Guide*, *18/1553-LZA 701 6014*, available from relevant WCDMA RAN CPI Library.

[14] *ENM Configuration Troubleshooting Guide*, 1/159 01-AOM 901 151-1

[15] *ENM Monitoring Troubleshooting Guide*, 1/159 01-AOM 901 151-2

[16] *ENM Performance Management Troubleshooting Guide*, 1/159 01-AOM 901 151-3

[17] *ENM Security Management Troubleshooting Guide*, 1/159 01-AOM 901 151-4

[18] *ENM on Cloud Backup and Restore Administrator Guide*, 5/1543-AOM 901 151

[19] *ENM Troubleshooting Guide*, 1/159 01-AOM 901 151

[20] *ENM Identity and Access Management System Administrator Guide*, 2/1543-AOM 901 151-1

[21] *ENM Network Security Configuration System Administrator Guide*, 2/1543-AOM 901 151-2

[22] *ENM Public Key Infrastructure System Administrator Guide*, 2/1543-AOM 901 151-3

[23] *OSS-RC Configuration for ENIQ*, 1/1546-AOM 901 076, available from Ericsson Network IQ Events CPI Library.

[24] *ENM Identity and Access Management Programmers Guide*, 19817-cna 403 3016

[25] *ENM Product Description*, 1/1551-AOM 901 151

[26] *ENM Monitoring System Administrator Guide*, 1/1543-AOM 901 151-2

[27] *LITP Node Hardening Instructions*, 2/1531-CSA 113 110

[28] *CAS Software Dropbox End-User Guide*, 6/1553-HSC 901 110, available from Ericsson Support.
[29] *ENM Neo4j Troubleshooting Guide*159 01-CNA 403 3405
[30] *ENM System Monitor User Guide*, 1/1553-cna 403 3115
[31] ENM NIG Connection Matrix
[32] *ENM System Security Configuration Programmers Guide*
1/19817-cna 403 3065 Uen
[33] *Neo4j Documentation*
https://support.neo4j.com/hc/en-us/articles/360006361794-Causal-Cluster-FAQ-for-heavy-workloads
[34] *ENM Parameter List*, 1/19059-AOM 901 151
[35] *Managed Object Model (MOM) RNC*, 155 54-CXC 173 5901/1-V1
[36] *SAPC, Measurements Ericsson Service-Aware Policy Controller User Guide*, 1/15553 - AXB 901 33/7
[37] *SAPC, Managed Object Model*, 155 54-LZN 708 0672/5-V1
[38] *ENM Privacy User Guide*, 2/1553-AOM 901 151